Published by CCDCOE

Cyber Threats and NATO 2030: Horizon Scanning and Analysis

A. Ertan, K. Floyd, P. Pernik, T. Stevens (Eds.)

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

KING'S College LONDON

WILLIAM & MARY
CHARTERED 1693

Published by CCDCOE

Cyber Threats and NATO 2030: Horizon Scanning and Analysis

A. Ertan, K. Floyd, P. Pernik, T. Stevens (Eds.)

CCDCOE
NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

KING'S College LONDON

WILLIAM & MARY
CHARTERED 1693

Cyber Threats and NATO 2030: Horizon Scanning and Analysis

ISBN (print): 978-9916-9565-0-2
ISBN (pdf): 978-9916-9565-1-9

COPYRIGHT AND REPRINT PERMISSIONS

NATO CCDCOE Publications
Filtri tee 12, 10132 Tallinn, Estonia
Phone: +372 717 6800
Fax: +372 717 6308
E-mail: publications@ccdcoe.org
Web: www.ccdcoe.org

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 29 nations providing a 360-degree look at cyber defence, with expertise in technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the Tallinn Manual 2.0, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise Locked Shields and hosts the International Conference on Cyber Conflict (CyCon), a unique annual event in Tallinn, joining key experts and decision-makers from the global cyber defence community. As the Department Head for Cyberspace Operations Training and Education, the CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. The Centre is staffed and financed by its member nations: Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

KING'S COLLEGE LONDON

King's College London is the fourth oldest university in England and provides world-class teaching in the heart of London to over 31,000 students from 150 countries. It has a distinguished reputation in law, the humanities, science—particularly health and medicine—and the social sciences, including international affairs. As King's approaches its 200th anniversary in 2029, it continues to encourage the critical thinkers, problem-solvers and change-makers the world needs to address its diverse challenges. Its School of Security Studies is dedicated to the understanding of security issues in an increasingly complex and uncertain world. Harnessing the depth and breadth of expertise across the War Studies and Defence Studies Departments, we are one of the largest communities of scholars in the world engaged in the teaching and research of all aspects of conflict, war, security and defence. Through our multi-disciplinary approach, we promote and value the study of security from different perspectives and methodologies. Our distinctiveness derives from the long history of King's College London as a university dedicated to the advancement of knowledge, learning and understanding of issues in the service of society.

WILLIAM & MARY

William & Mary, in Williamsburg, Virginia, carries on an educational tradition that traces back more than three centuries. As the second-oldest institution of higher education in the United States, William & Mary was founded by King William III and Queen Mary II of England as an American overseas campus representing the British Crown. Known as the alma mater of globally-renowned historical figures such as George Washington, Thomas Jefferson, James Monroe and John Marshall, William & Mary today is a leading force for international education and training ground for international specialists around the world. William & Mary boats more than 40 undergraduate programs and more than 40 graduate and professional degree programs, attracting students from 50 states and more than 60 foreign countries.

The mission of the William & Mary Whole of Government Center of Excellence is to train a new generation of future leaders who have hands-on, practical experience working across the different organizational cultures. These leaders must harmonize to facilitate true interagency collaboration— long before finding themselves forced to deal with such issues during a foreign deployment or national emergency. The work of the Center is primarily focused on training, education, and research related to interagency collaboration, complex national security challenges, and other public policy problems for mid-career policy professionals and military officers. The Center also brings together leaders from all levels of government and the military for symposia, discussions, and projects to promote creative, collaborative solutions to emerging issues.

Disclaimer

TABLE OF CONTENTS

FOREWORD

Many things of profound historical importance happened in the Western alliance in 2016. Voters in the United Kingdom and the United States confounded expectations by voting, respectively, to leave the European Union and elect a businessman with no previous governing experience as President. North Korea gave its most overt indications to date of the extent of its missile arsenal. Turkey saw off an attempted coup. International terrorism struck several European countries. More positively, for the purposes of human development, the proportion of the world connected to the internet passed the half-way point.

Yet for the Western alliance, one relatively unnoticed, but strategically crucial, development that took place in the rarefied atmosphere of international summitry may have some of the most important strategic ramifications. In Warsaw, in July of that year, NATO formally recognised cyberspace as a domain of operations for the political and military alliance. This necessary recognition – that mutual defence and the ability to operate in this entirely artificial human creation was now vital for the security of an alliance of free societies – reflected the remarkably rapid development of cyberspace in a few short decades.

The Warsaw declaration reflected the now obvious truth that, in the words of the communique, 'cyber defence is a part of collective defence' (NATO, 2016). It also reflected that NATO countries, and the alliance as a whole, would need to develop and be able to deploy capabilities. But in its own note, issued at the time, a NATO CCDCOE researcher rightly concluded that what this would mean in practice would be 'difficult to decode' (Minárik, 2016). There are two reasons for that. First, as well as being a contested domain of operations, cyberspace is, by and large, a civilian and private sector-led domain of largely peaceful and often commercial activity. Many of the main changes in cyberspace are not driven by governments at all, let alone those parts of governments primarily concerned with security. Second, the technologies driving behaviour in cyberspace continue to develop at an astonishing rate.

So, this book is timely and vital and will be welcomed by many in government, business, academia and civil society as an excellent contribution to 'decoding' what it means for a political and military alliance of free societies to deal collectively with cyber threats. It is a hugely positive contribution to 'decoding' the historic Warsaw communiqué of 2016.

How that declaration is implemented in the next decade is one of the most vital challenges of the 2020s. Technology has been essential to getting through the coronavirus pandemic and we depend on it now, more than ever. Although technology has held up heroically in the face of increased demand, we have yet to fix the security of the technology we currently have, let alone the technologies of the future. None of Russia, Iran or North Korea have an alternative vision of technology nor the means to deliver one. They

operate on the internet built by the West. But they—especially Russia—excel at exploiting weaknesses in that free and open internet. So too do lawless, well-organised groups of transnational cyber criminals. Organising our defences better, disrupting the ability of hostile actors to harm us, and getting the right threat intelligence to the right people at the right time, remain as important now as half a decade ago.

China is different. It has been described by the Secretary General of NATO as 'not our adversary' but as a nation 'that does not reflect fundamental human rights and tries to intimidate other nations' (Stoltenberg, 2020). In the cyber domain, as well as exploiting the same weaknesses as the likes of Russia, China is building an alternative, more authoritarian model of technology. Moreover, China has publicly articulated a strategy to become the leader of many of the most important technologies of the future. In doing so, China has helped transform our understanding of cyberspace as a domain of operations. It is not just a domain we need to defend and in which we must operate when necessary; it is a domain where we need to have confidence in the quality and security of the technology we are using.

But there are other critically important reasons for looking hard at how new technologies require a new security response. We cannot predict with any confidence who will seek to exploit the weaknesses of new technology over the long term. But someone will. So safer, more resilient and more secure technology is now an imperative.

This matters for all aspects of our societies. Technologies that matter for warfighting also matter for civilian life. The contents of this book bring that out well. Developments like 5G and artificial intelligence, or their practical application in areas like smart cities, are not driven by military requirements but by the opportunities they offer to the lives of our citizens. Securing them has to be done in a way that is compatible with their use in free societies.

Special protection will continue to be needed to secure military capabilities, and specialist capabilities will be needed for the responsible use of military power. Governments are already working towards better organisation of their cyber capabilities but these efforts must be ongoing and persistent. All of this will need to be done in a way consistent with safer technology.

Whether it is 5G, machine learning, blockchain, quantum, or some other new technology, a real opportunity presents itself. The previous generation of technology came into being with little thought for security. That was no-one's deliberate decision; it just happened that way. As a result, we ended up with an ecosystem where the price of entry for free, web-based services was the surrender of personal data. This makes us vulnerable. We are some way off outright cyber conflict, but we are in a constant state of what might be called 'cyber-harassment'. Authoritarian countries in particular are taking advantage of our openness, knowing that like-for-like retaliatory measures against them will have less impact on their more closed societies.

Now is the time to fix those vulnerabilities, as new technologies appear. The Internet of Things may, on one metric, increase our vulnerability because it increases the number of internet-connected devices and the range of activities they afford and upon which we depend. But they also involve physical products where we can specify, as we do in other areas of civilian and military life, what standards they must meet to be secure.

We cannot and should not lock down or weaponise cyberspace. We must, of course, continue to defend cyberspace and operate in it effectively. And we can, and must, secure the next generation of technologies. Doing so embeds the advantages of the free and open societies represented within the NATO alliance.

That is what cyberspace as a domain of operations must surely mean. This book is a valuable resource in helping us further develop our thinking on this key issue for NATO and its mission to defend and promote freedom, security and democratic values.

Ciaran Martin
Professor of Practice in the Management of Public Organisations
Blavatnik School of Government
University of Oxford

REFERENCES

NATO. (2016) *Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*. 9 July 2016. Press Release (2016) 100. Available from: https://www.nato.int/cps/en/natohq/official_texts_133169.htm [Accessed 1st December 2020].

Minárik, T. (2016) *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit*. NATO CCDCOE. Available from: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/ [Accessed 1st December 2020].

Stoltenberg, J. (2020) *Online pre-ministerial press conference by NATO Secretary General Jens Stoltenberg ahead of the meetings of NATO Ministers of Foreign Affairs.* North Atlantic Treaty Organisation. 30th November 2020 Available from: https://www.nato.int/cps/en/natohq/opinions_179791.htm [Accessed 1st December 2020].

INTRODUCTION

All members of NATO benefit greatly from digital connectivity and the many opportunities it provides for social, economic and political development. At the same time, it is widely recognised that heightened dependency on digital networks and systems is a systemic vulnerability that can be exploited by a wide range of criminal and strategic actors. The community of like-minded democracies gathered under the NATO umbrella is therefore being challenged as never before by diverse and dynamic cyber threats. This volume looks ahead to how NATO can best address these issues over the next decade, contributing to the conversation begun by Secretary General Jens Stoltenberg in June 2020. In launching the NATO 2030 initiative, the Secretary General canvassed input from a wide range of stakeholders about how to strengthen NATO militarily and politically in a turbulent and competitive world (Stoltenberg, 2020; NATO Science and Technology Organization, 2020). This volume engages directly with that discussion and aims to stimulate broader debate on the future operational environment from the perspective of cyber threat horizon-scanning and analysis, with particular attention to the impact of new and emerging technologies.

In the period under consideration, NATO's technological edge will be increasingly challenged. Recent work by NATO has highlighted the wide range of emerging and disruptive technologies which may negatively impact international security and stability and the ability to promote democratic norms (NATO Science and Technology Organization, 2020). In May 2019, the Secretary General warned that new technologies such as artificial intelligence and machine learning will render cyber threats even more pernicious, as well as potentially altering the nature of warfare (Stoltenberg, 2019). NATO is fortunate to be already deeply invested in addressing these issues. The Cyber Defence Pledge (2016), for instance, exists in part 'to ensure the Alliance keeps pace with the fast-evolving cyber threat landscape' and reasserts a collective will to tackle cyber threats extending as far back as the 1990s (NATO, 2016; Burton, 2015). This includes successive Strategic Concepts recognising the critical importance of cybersecurity to NATO's missions and military operations. Since 2016, NATO has bolstered its existing outreach and engagement programmes and embarked upon new ones, all geared to improving its cybersecurity and that of its member states.

As recognised by NATO, however, more work is required to understand the evolution of the cyber threat environment. This was emphasised in the Strategic Foresight Analysis of NATO Allied Command Transformation, which encouraged NATO to 'develop capacities to detect both subtle and seismic changes in the information environment and understand them on local, operational and global levels' (NATO Allied Command Transformation, 2017: p. 51). The Cyber Defence Pledge itself aims to 'improve our understanding of cyber threats, including the sharing of information and assessment' (NATO, 2016). In this context, Alliance political and strategic leaders need to improve their understanding of cyber threat vectors; actors' objectives,

intent and capabilities; and the future cyberspace operational environment across all phases and contexts. This includes peacetime conditions, targeted cyberspace operations with disruptive or even lethal impacts, and kinetic warfighting in conjunction with destructive cyber attacks. In addition, cyber threat intelligence (CTI) must be comprehensible and operationalised to support strategic-political decision-making.

The present volume addresses these conceptual and practical requirements and contributes constructively to the NATO 2030 discussions. The book is arranged in five short parts, beginning with 'Cyberspace Adversaries and NATO's Response'. This part opens with two papers on Russian internet and cyber capacity. **Juha Kukkola** explores the strategic implications of Russian plans for a closed national network, identifying defensive and offensive advantages for Russia in the structural asymmetries thereby promoted. **Joe Cheravitch** and **Bilyana Lilly** draw attention to the constraints on Russian cyber capacity caused by domestic recruitment and resourcing issues and suggest how NATO might be able to leverage these limitations for its own cybersecurity objectives. **Martin C. Libicki** and **Olesya Tkacheva** offer a novel perspective on cyber conflict with an adversary like Russia, analysing the possibilities for horizontal escalation into other domains as well as in-domain vertical escalation, and the consequences for NATO doctrine and risk management.

Part two, 'New Technologies and NATO's Response', opens with a chapter on 5G by **Luiz A. DaSilva**, **Jeffrey H. Reed**, **Sachin Shetty**, **Jerry Park**, **Duminda Wijsekera** and **Haining Wang**. The authors propose a series of measures that NATO and its partners can implement to secure 5G technologies and their supply chains, including forms of risk management, standardisation and certification that will maximise the military and social benefits of this new generation of mobile systems. Using an extensive horizon-scanning database, **Jacopo Bellasio** and **Erik Silfversten** identify a range of new and emerging technologies likely to shape the future cyber threat landscape and propose ways in which NATO can prepare for and adapt to these eventualities. **Simona R. Soare** and **Joe Burton** demonstrate the vulnerabilities of hyperconnectivity through the hypothetical scenario of a smart city under concerted cyber attack, drawing out the lessons NATO must learn about the relationship between local and supranational security under hi-tech conditions.

Part three, 'Warfighting, the Cyber Domain and NATO's Response', contains two chapters concerned with Multi-Domain Operations (MDO), the warfighting concept being adopted across NATO. **James Black** and **Alice Lynch** explore the implications of MDO's networked dependencies and how adversaries are hoping to exploit these, proposing that NATO needs to better understand the interplay of external threats and internal vulnerabilities to combat cyber threats to multi-domain activities. **Franz-Stefan Gady** and **Alexander Stronell** conduct a comparative analysis of NATO Allies' integration of cyber capabilities with kinetic operations in MDO and offer proposals for improving NATO performance in a future high-intensity conflict with a

near-peer competitor.

Part four, 'Information Sharing, Cyber Threat Intelligence and Exercises', begins with a view from the cybersecurity industry by **Michael Daniel** and **Joshua Kenway** of the Cyber Threat Alliance. They offer a programme for the sharing of CTI between NATO and its stakeholder community that seeks to correct some of the faulty assumptions built into existing CTI frameworks. **Chon Abraham** and **Sally Daultrey's** comparative analysis of CTI sharing in Japan, the US and UK suggests that national contextual factors can inhibit this critical cooperative function and proposes a series of organisational changes to remedy this condition. **Andreas Haggman** makes a distinct methodological contribution to the NATO cybersecurity discussion with its promotion of wargaming as a tool for imagining and anticipating conflictual futures in their diverse social, political and technical dimensions.

Part five looks at 'Regulatory and Policy Responses to Cyber Security Challenges'. **Cindy Whang** focuses on how export control regimes should be reinvigorated to accommodate cybersecurity concerns across the Alliance. **Laurin B. Weissinger** concludes the volume with an appeal to improve NATO's understanding of networked complexity, including through threat and attack modelling, to provide more effective and tailored cybersecurity solutions.

All the chapters in this book have undergone double-blind peer review by at least two external experts. We thank all our reviewers for their timely and constructive comments and for guaranteeing the academic quality of the work presented herein.

A. Ertan, K. Floyd, P. Pernik, T. Stevens

REFERENCES

Burton, J. (2015) NATO's cyber defence: Strategic challenges and institutional adaptation. *Defence Studies*. 15 (4), 297-319. DOI: 10.1080/14702436.2015.1108108.

NATO. (2016) *Cyber Defence Pledge*. Available from: https://www.nato.int/cps/en/natohq/official_texts_133177.htm [Accessed 17th November 2020].

NATO Allied Command Transformation. (2017) *Strategic Foresight Analysis: 2017 Report*. Available from: https://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf [Accessed 17th November 2020].

NATO Science and Technology Organisation. (2020) Science and Technology Trends 2020-2040: Exploring the S&T Edge. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf [Accessed 17th November 2020].

Stoltenberg, J. (2019) *Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference*. [Speech]. London, 23rd May. Available from: https://www.nato.int/cps/en/natohq/opinions_166039.htm [Accessed 17th November 2020].

Stoltenberg, J. (2020) *Remarks by NATO Secretary General Jens Stoltenberg on launching #NATO2030 – Strengthening the Alliance in an increasingly competitive world.*

[Speech]. Brussels, 8th June. Available from: https://www.nato.int/cps/en/natohq/opinions_176197.htm [Accessed 17 November 2020.].

PART I:
Cyberspace Adversaries and NATO's Response

The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry

Juha Kukkola
Captain, Doctor of Military Sciences
Department of Warfare
Finnish National Defence University

Abstract: The Russian Federation is constructing a closed national network. If successfully completed, this state-controlled, technologically independent, and self-sufficient segment of the internet can be disconnected from the global internet by 2024. The segment is based on a national system-of-systems of information security and defence that will protect the Russian regime against internal and external information threats. It will also provide a source of power in the ever-continuing great power struggle and even a decisive advantage on a strategic level in the cyber domain. This chapter demonstrates that the Russian project is an effort to shape cyberspace through state action on a strategic level to gain an asymmetric military advantage. The advantage is based on the differences in freedom of action, common operational picture, command and control and resilience between one nation closing its networks and other nations leaving their networks open and their critical information infrastructure unprotected. These differences create strategic-level structural cyber asymmetry which can influence the way force is used in a state-to-state conflict. This chapter provides new insight on how a closed national network, or the Russian national segment of the internet, in particular, could change the balance of power and the rules of play in the future cyber domain.

Keywords: *Russian Federation, cyber defence, closed national network, asymmetry*

1. INTRODUCTION

The Russian Federation is constructing a national segment of the internet (*natsional'nyi segment interneta*) which can be disconnected from the global internet when certain threats materialise (FZ-90, 2019). This project is incorporated in the 2017 National Programme of the Digital Economy, which aims to achieve 'digital sovereignty' by 2024 (RP-1632, 2017). If successful, the programme will put the Russian part of the internet under the control of the Russian state. Although some commentators have argued that the Russian regime's project is mainly about authoritarian domestic political control over the internet, the project also has a military aspect that can affect the international balance of power (Soldatov, 2017; Ermoshina & Musiani, 2017; Vendil-Pallin, 2017; Nocetti, 2018). The concept of the Russian national segment of the internet is based on strategic-cultural Cold War-era Soviet ideas which carried with them a promise of an asymmetric advantage in great power relations (Kukkola, 2020). The project also contributes to the fragmentation of the internet along national boundaries, which is becoming ever more evident (Drake, Cerf & Kleinwächter, 2016).

Kukkola, Ristolainen and Nikkarila (2017) have argued that the Russian national segment of the internet will become a closed national network, which will provide an asymmetric advantage against states leaving their networks open. This advantage is based on the restructuring of cyberspace or, in military terms, the shaping of electronic battlespace on a strategic level. This chapter develops this argument further by arguing that the presence of structural cyber asymmetry can be analysed through the differences of freedom of action, common operational picture (COP), command and control (C2) and resilience between a nation closing its networks and nations leaving their networks open. These variables capture the essential characteristics of cyberspace on an operational-strategic level. At a strategic level structural cyber asymmetry will affect the way force is used in future state-to-state conflicts, contribute to the fracturing of cyberspace into national segments, and even promote a cyber arms race.

This chapter presents a case study where the Russian national segment of the internet and a theoretical open national network are analysed to explain the phenomenon of structural cyber asymmetry. In the first part, Russia's reasons for and means for constructing a national segment of the internet are examined. In the second, the concept of structural cyber asymmetry and related concepts of freedom of action, COP, C2 and resilience are explained. The third part examines the differences between the Russian segment, or a closed national network, and a Western open national network. In the fourth part, a qualitative analysis of Russia's closed network and a theoretical open network is conducted, examining the relative advantages and disadvantages of open and closed network nation defenders in the context of cyber conflict. Advantages and disadvantages are analysed to demonstrate the presence of structural cyber asymmetry and to understand its nature. Finally, the chapter will conclude with a discussion on the military-strategic implications of structural cyber asymmetry.

2. WHY RUSSIA IS PURSUING ASYMMETRY IN CYBERSPACE

To understand Russia's objectives and structural cyber asymmetry some basic concepts need to be introduced. First, a closed national network is a theoretical concept which describes a national network that can be disconnected from the global internet and still function normally in providing communications for the state administration, national economy, civil society and the military. An open national network is a theoretical state network based on the current Western way of managing the internet. Second, the Russian national segment of the internet is a real-life case of a closed national network. It consists of the internet infrastructure and other networks and systems residing in Russia and under its sovereign legal powers. It defines the borders of cyberspace and is a political, administrative and legal concept. Third, a unified information space (*edinnoe informatsionnoe prostranstvo*) is a strategic-cultural idea, which makes it understandable and reasonable for the Russia regime to develop the Russian national segment of the internet. The idea describes how this segment of cyberspace should be arranged according to cybernetic principles. Fourthly, a national system-of-systems of information security and defence is a collection of interconnected means and methods of the state to delineate, protect and control its national segment. The system-of-systems protects the state and its sovereignty and functions as a source of national power. In its ultimate state, as a manifestation of unified information space, it incorporates the whole national segment of the internet. All these concepts, except the first, are based on the thinking of Russian civilian and military academia. It should also be noted that the commonly used term, 'Russian internet' or 'RuNet', refers to the Russian-language social and cultural online environment which developed in the 1990s and 2000s without state interference. Its borders do not correspond to Russia's state borders and Russia is not currently claiming sovereignty over it.[1]

The Russian state began to build a national segment of the internet in the early 2010s because it was rational from the point of view of decision-makers (Kukkola, 2020; Nocetti, 2018; Kari, 2019). The idea of information sovereignty (*informatsionnyi suverenitet*) was present in Russian political discourse by the early 2000s and was promoted as a counterforce to a perceived American hegemony in internet governance and information technology superiority. Between 2009 and 2011 it became clear to the Russian regime that RuNet had transformed into an independent platform of political mobilisation. This was perceived as a threat to its authoritarian regime. Incidentally, the KGB-minded Russian security services had argued for the control of the internet since the mid-1990s (Thomas, 1998). After 2011 the regime began to implement political control and censorship of RuNet through laws and decrees. Meanwhile, it became apparent to Russian political and military elites that cyberspace would be militarised and that critical information in-

[1] For a more comprehensive discussion on these concepts see Kukkola, Ristolainen & Nikkarila, 2017; Ristolainen & Kukkola, 2019; Kukkola, 2020.

frastructure would be targeted in the next large-scale or regional war (Kukkola, 2020).

Autumn 2014 was a turning point for the Russian regime. A definite change in the strategic environment led the regime to pursue a centralised control of the internet under the guise of 'the national segment of the internet' which itself was a product of the ideas of information sovereignty and unified information space. According to these ideas, the state must control its information space and its borders to achieve information sovereignty.[2] Consequently, unified information space is a model for constructing such a space around vertically and horizontally integrated state-controlled networks and automated C2 management systems. This kind of national information system would provide an asymmetric response (*asimmetrichnyi otvet*) against an enemy by denying it an attack surface and making national systems more resilient while leaving Russia free to operate against an adversary (Kukkola, 2020; Pynnöniemi, 2018). The concept has its roots in the Soviet response to Reagan's Strategic Defense Initiative (SDI) in the 1980s (Hoffman, 2009). Arguably, Russian actions were influenced by multiple threats that seemed to materialise in 2014–2015. The global balance of power was changing as China rose to challenge the US while Russia's relations with the West became antagonistic. The Russian regime perceived itself to be vulnerable to 'colour revolutions' and to new technological threats in the information, cyber and space domains. Russia had also failed to create international cyber and information security norms to control its more advanced adversaries. The Russian strategic cultural ideas and the Chinese example of 'the Great Firewall' offered a possible solution that the Russian regime embraced.

Between 2015 and 2020 the Russian regime adopted multiple laws, strategies and programmes which were designed to establish a national segment of the internet, protect it from internal and external threats and create power. These policies have sought to establish a truly independent, self-sufficient, competitive, integrated, resilient and secure Russian national segment of the internet. The programmes have already produced several components: a national cyber incident management system (GosSOPKA), a national centralised system for monitoring and managing telecommunication networks (TsMUSSOP), a federal government information management system (Upravlenie), a national network of situation centres and other centralised management networks including national energy and defence industry manage-

[2] According to an official Russian definition information space or environment is 'a set of information resources created by subjects of the information sphere, means of interaction of such subjects, their information systems and the necessary information infrastructure' (Ukaz-203, 2017). The information sphere is a larger entity also encompassing the subjects of information sphere (i.e. users and organisations) and the rules and norms regulating their interaction (Ukaz-646, 2016). Conversely, according to US Joint Doctrine the information environment is the aggregate of individuals, organisations and systems that collect, process, disseminate or act on information. This environment consists of three interrelated and interacting physical, informational and cognitive dimensions (JP 3-13, 2014: p. ix-x).

ment systems (Kukkola, Ristolainen & Nikkarila, 2017; Kari, 2019; Kukkola, 2020). Russia aims to develop domestic hardware, software and artificial intelligence industries to a scale that will achieve 'technological sovereignty', or self-sufficiency in the ICT sector (Thornton & Miron, 2020). However, this ambitious programme has technological challenges (Dear, 2019). It has suffered from the resignation of the Russian government in January 2020, from the fall of global oil prices and the COVID-19 crisis. The resistance of civil society and the private sector has also been significant. Consequently, President Putin apparently agreed to postpone the programme until at least 2030 (Ukaz-474, 2020).

Russian state policies resonate with the ideas of Russian information warfare (IW) theorists who have argued for the development of a national information defence or management system since the early 2000s (Kukkola, 2020). These ideas are based on a shift in the Russian perception of the character of war, which has evolved incrementally towards a version where the borders between war and peace become increasingly blurred. The will of the population and its decision-makers and the national economy have become the primary military-political targets. This means that state control of the national information space is necessary for succeeding in the continuous great power, zero-sum struggle (Thomas, 2017; Jonsson, 2019; Kukkola, 2020). Thus, the shaping of cyberspace has a critical role in deterrence and strategic-level preparations of the battlespace. However, although the Western and Russian ideas about cyber security are converging, controlling the substance and flow of information is still the primary concern of the Russian concept of information security. During the late 2010s, Russia adopted the concept of critical information infrastructure as an object of national security. The concepts of integrity, resilience and security of the Russian part of the internet have been adopted to define the security of information-technological communication systems (FZ-126, 2003; Sheremet, 2019), and the Russian leadership routinely discusses cyber threats (Latukhina, 2018). If Russian policies and the ideas of IW theorists merge fully, the result will be a national system-of-systems of information security and defence which will protect and control the national information space from psychological and technological information threats—and incorporate that space altogether.

3. STRUCTURAL CYBER ASYMMETRY

Human action can change cyberspace in ways that it cannot change other domains. Cyberspace is an information technology-based man-made global domain governed by humans in the information environment. It is an environment in and through which power can be used in ways guided by ideas and beliefs. Through certain resources at their disposal, states can control and shape cyberspace and thus change its characteristics and properties. Cyberspace is a new and constantly evolving environment with unknown or poorly understood potential threats. Consequently, states shape cyberspace in distinct ways guided by strategic-cultural ideas and according to the resources at their disposal.

The military-strategic importance of the shaping of cyberspace through constructing closed national networks or real-world national segments is based on the possibility of creating asymmetry (Kukkola, Ristolainen & Nikkarila, 2017). Without asymmetry, national segments would only make sense as instruments of domestic political control and protectionist economic policies. However, the traditional view of cyberspace asymmetry based on either the difficulty of attribution, disproportionate capabilities of non-state actors, non-traditionality of cyber means, or the advantages of cyber offence over defence is too narrow (Liff, 2012; Gartzke, 2013; Rid & Buchanan, 2015). By contrast, structural cyber asymmetry is a property of cyberspace which emerges between two actors when the structure and rules of cyberspace are shaped so that one of them gains a disproportionate and exploitable defensive and offensive advantage.

Kukkola, Ristolainen and Nikkarila (2017) have argued that when a nation manages to close its networks and build defensive lines inside this national network it will gain an asymmetric advantage in Computer Network Attack and Exploitation operations (CNA/CNE) against a nation that leaves its national networks open in a state-to-state conflict. The argument is that it is easier for a nation closing its networks to attack and defend than it is for an open network nation. This is because the nation closing its networks can minimise its attack surface, build defence in-depth and control the network centrally while the nation leaving its networks open is vulnerable through multiple attack vectors.

In previous studies (Kukkola, Ristolainen & Nikkarila, 2017) the concepts of freedom of action, situational awareness and decision-making have been used to analyse the advantages and disadvantages of closed and open networks in CNA/CNE operations. This approach was based on a theoretical operational-strategic level analysis. Technical issues were not analysed, although practical issues of disconnecting national networks have been examined by others (Kukkola, Ristolainen & Nikkarila, 2019). This chapter argues that it is advantageous to replace situational awareness with a COP and decision-making with C2 when analysing structural cyber asymmetry. Freedom of action needs to be disconnected from its geographical connotations and resilience, understood as a property of cyberspace, should be added to complement this analysis. These modifications direct the analysis to the effects of the structure of cyberspace instead of the subjective processes of decision-makers—which in the context of national security are often unknowable to the temporary outside observer.

Freedom of action, COP, C2 and resilience are relative variables whose differences demonstrate the presence of structural cyber asymmetry. In the context of this chapter, these concepts refer to technological, organisational and functional properties of closed and open networks, not to the capabilities of national cyber forces. Freedom of action refers to the ability to act in a certain domain while at the same time possessing an ability to deny adversaries

that same capability. In cyberspace, this ability is tied to user privileges and connections, not to geographical continuity (Kiviharju, Huttunen & Kantola, 2020). Moreover, traditional material calculations of the correlation of forces lose their meaning as 'forces' are not positioned against each other (Kallberg & Cook, 2017). Physical destruction is replaced by affecting the performance capacity of the targeted system (NATO, 2020). Thus, the objects of the analysis of freedom of action are the effects of the borders and internal structures and processes of closed and open networks on the ability of actors to affect systems, processes, or adversary's operations in either own or enemy networks.

Because the concept of situational awareness refers to a personal and unique comprehension of the situation (Endsley, 2015), it is difficult to capture when analysing strategic-level cyber conflict. However, because information superiority is based on accurate and current situational awareness, it is necessary to somehow capture its effects in the analysis of structural cyber asymmetry. The ability to detect and be aware of the situation in both one's own and in adversary networks is central to cyber warfare as the ability to know is the precondition of the ability to act (Brantly, 2016). The COP can be defined as analysed, organised and continuously updated information about the situation in an area of operations that is available to one or more actors (Kuusisto, Kuusisto & Arminsted, 2005). Consequently, when analysing COP as a precondition of national cyber situational awareness in the context of structural cyber asymmetry, the objects of analysis are the structures, processes, information content, models and flows related to offensive or defensive cyber operations (MNE7, 2012). Advantages in these factors facilitate faster, more efficient and effective decision-making (Simon, 1997).

Analysis of decision-making at the operational-strategic level is difficult because, like situational awareness, it is a partly cognitive, partly social phenomenon, emphasising subjective agency and competence and, in the case of cyber operations, it is also highly secretive (Howard & Abbas, 2015). However, the concept of C2, defined as a process of planning, preparing, decision-making, executing, directing, coordinating and evaluating to achieve a certain objective in the context of certain technological and organisational systems and structures, can be used to examine the presence of structural cyber asymmetry with the evidence available (Hayes & Alberts, 2005; Elbanna, 2006). Because the characteristics of cyberspace directly influence C2 (Brantly, 2016; Chen, 2019), the object of analysis is not the process of decision-making according to some specific model but rather the systems of information management, decision support and execution and the structures of the national networks (O'Brien & Marakas, 2011). Thus, structures, processes and technologies are evaluated according to their effects on the speed of decision-making, the exactness of execution and overall control interpreted as effectiveness.

Resilience, as the last variable used to analyse the presence of structural cyber asymmetry, directs the attention to the infrastructure of cyberspace.

Although resilience is a somewhat contested concept (Humbert & Joseph, 2019), cyber resilience can be defined as 'the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources regardless of the source' (Ross et al., 2018: p. 1). While freedom of action is used in this chapter to analyse the active ability to affect the adversary's systems or protect own systems, resilience captures the passive protective, risk-minimising and continuity-enabling policies and systems affecting the properties of the information infrastructure (Libicki, 2016). Thus, the object of analysis in the case of resilience are those systems and policies that ensure the continuity of the critical information infrastructure on a national level and its adaptation to new threats.

4. CLOSED AND OPEN NATIONAL NETWORKS

Based on the writings of Russian theorists and official policy documents, the Russian closed national network, or the Russian segment of the internet, is approached in this chapter as a national system-of-systems of information security and defence. A system-of-systems is composed of multiple subsystems, the interactions of which enable the achievement of a goal which no individual subsystem can achieve alone (Ackoff, 1971). The goal, in this case, is national information security, which is understood as protecting the state from external and internal information (technological and psychological) threats to ensure its sovereignty, territorial integrity, economic development, defence and security (Ukaz-646, 2016). For Russia, and incidentally also for China, information threats are categorised into the military-political use of information weapons, terrorism, crime, the efforts to use a dominant position in the information space to cause damage to others, disseminating harmful information to the political, social, economic, spiritual and cultural systems of other states, and threats to the global information infrastructure (SCO, 2009; RP-788, 2015). The system is a complex system-of-systems as its subsystems have their own functions and management mechanisms that are somewhat independent. Subsystems can function in unpredictable and inefficient ways (Thurner, Hanel & Klimek, 2018). The subsystems should be understood as political, governance, normative, organisational, economic, technological and security and military entities. They have been formed through soft systems methodology and are thus observation-based theoretical constructs (Checkland, 1993). The subsystems are explored more comprehensively elsewhere and here it is only possible to offer a summary of each.[3]

There are seven subsystems in the Russian system-of-systems, which are classified according to borders (parts), functions, principles or rules and ob-

[3] The original model was presented in Kukkola (2020). It has been modified for this text by introducing 'active counter measures' subsystem and incorporating a previous subsystem of cyber diplomacy into it. On active counter measures, see Blank, 2013; Giles, 2016; and Ajir & Vaillant, 2018.

jectives.[4] The first is the scientific-industrial basis of the state. It is based on import substitution policies and significant state investment in technology and science. Direct state ownership of strategic assets is common. This subsystem's objective is to produce the scientific-technological and knowledge aspects of a state's cyber power.[5] The subsystem contributes to the goal of national information security by directly shaping cyberspace, protecting the supply chain and providing security through obscurity and transparency as Russian produced hardware and software (HW/SW) are accessible to security services and the military through backdoors.

The second subsystem is state authentication and encryption. It is based on domestically produced and operated services and algorithms that are controlled directly or indirectly by the state. Use of the subsystem is mandatory for public services and state corporations, and it is forced on the private sector and private users. The subsystem's objective is to make all data traffic inside Russian borders transparent to the security services and the military and to protect data from foreign exploitation.

The third subsystem consists of the administrative and technological processes of blacklisting and content management through removal and restriction. The state publishes a database of unwanted sites and addresses and service and content providers are legally bound to restrict access to those on this blacklist. This system includes vigilante groups and self-censorship. The objective of the system is political control through the removal of subversive information.

The fourth subsystem consists of the targeted surveillance systems and the massive internet data traffic localisation and retention conducted by the internet Service Providers (ISP) as ordered by the state. The subsystem is based on massive, distributed data centres and networked monitoring systems and provides a collection of information and its analysis. It is highly centralised and its objectives are mainly counterintelligence, law enforcement and political control. The second, third and fourth subsystems contribute to information security by making the flow and content of data accessible to security services and the military.

The fifth subsystem consists of the Critical Information Infrastructure (CII) and the regulations and policies related to it. The subsystem is based on state ownership or indirect control of CII and legal obligations on private actors to protect it. It includes backups of top-level domain name servers, routing registers and internet Exchange Points (IXP). The subsystem enables the functioning of the national segment and its disconnection from the global

[4] Military networks and systems are separate but interdependent parallel system, which are not discussed in thischapter. They are a subcomponent of CII.

[5] Cyber power is an ability that empowers an actor to influence others in or through cyberspace and to control and shape cyberspace to its advantage according to its preferences. Resources of power consist of human knowledge, technology, regulations and organisations (Kukkola, 2020).

internet, thus contributing to information security.

The sixth subsystem is based on active information-technological and information-psychological countermeasures. The subsystem is managed by state-controlled or affiliated news services and educational, patriotic and religious institutions. It also includes dedicated cyber diplomacy organisations and cyber espionage and warfare units of the security services and the military. It controls the domestic information environment by controlling the substance of information and conducts external overt and covert espionage, influence and cyber operations abroad to prevent possible threats from emerging. The subsystem also increases information security by attempting to norm-bound (entangle) potential adversaries and, thus, restricting the information superiority of advanced adversaries. If successful, it might for example create taboos concerning the offensive use of cyber capabilities.[6]

The seventh subsystem consists of feedback, monitoring, control and management systems. It is managed by the state and security services and includes national-level cyber training ranges and exercises. This subsystem provides the vertical control and horizontal integration of the closed national network. The different systems penetrate all nationally significant networks. The subsystem provides information on the national segment and the whole society, in essence a real-time analysis of all information threats, not just cyber, and enables control of information flows in the segment and at its borders. Its objective is to ensure national information security through monitoring, controlling and defending the national segment of the internet.

These subsystems are based upon the Russian project to construct a national segment of the internet. Conversely, a generic open national network is, in this chapter, loosely based on the way the internet was governed in the technologically advanced Western countries in the mid-2010s.[7] This time and region were chosen as the basis of the open national network because Russia formed the basic principles of its project to build a national segment in contrast to the way the internet was managed in the West at that time. The Russian project is a response to the weaknesses and strengths perceived in those Western models at the time of writing of the information security doctrine and the National Programme of the Digital Economy in 2015–2016. Although, the US is the most obvious competitor and even an adversary of Russia, the open national network model is not solely based on the US example of a national network. This is due to the US's unique relationship to the internet, and the US's disproportionate economic and scientific-technological power in relation to other Western powers.

Therefore, using the US model of national network as an example would obscure the fact that the other Western countries are dependent on US software

[6] On the dissuasive, soft or diplomatic use of cyber power, see Nye (2017).

[7] Sources used to induce the properties of an open national network: include ITU, 2015; ENISA, 2015; Hitchens & Goren, 2017; European Commission, 2020; NATO CCD COE, 2020 and; Tikk & Kerttunen, 2020.

and hardware. Thus, the comparison offered below is designed to highlight the potential asymmetric effects of the policy pursued by Russia vis-à-vis regional Western powers if they do not drastically change their internet governance policies. Structural cyber asymmetry affects both small and great powers and can affect great powers through their allies. It is, however, recognised that after 2016 the Western cyber security strategies and capabilities have begun to change (e.g. NATO, 2016) and this will be noted and discussed below.

Although an open national network is arguably not a system-of-systems in the sense of a national information security and defence system, it is approached below through the subsystems of the Russian national system. These subsystems capture almost all technological, administrative, economic, normative, political and security aspects of a territorially delimited part of cyberspace. This approach helps to conceptualise national networks as more than just a technological phenomenon and to compare them even when they differ from each other. Moreover, when national networks are modelled as systems their interaction, competitive or confrontational, can be analysed. There is, therefore, an element of simplification explicitly present in the model but its function is to underline the differences between two types of networks. Table I shows the main differences between a closed and open national network.

Table I: Closed and Open National Network

Subsystems	The Type of Network	
	Closed National Network	Open National Network
1. Scientific-technological basis	• State-led • Closed markets, corruption and red tape • State ownership of strategic assets - foreign ownership highly regulated • Domestic SW/HW ecosystem • Primarily proprietary source code • Few international interdependencies • Limited international cooperation in cyber security	• State participation varies • Open markets • Privatization of strategic assets - foreign ownership regulated • Few domestic SW/HW • Fractured field of international and domestic services suppliers • Significant foreign interdependencies (supply-chains)
2. Authentication and encryption	• Primarily domestic SW/HW solution • State certification required for all cryptography • State able to decrypt all traffic without administrative process	• Limited domestic solutions • State provides certification for official use and recommendations • Slow decryption because of political and legal issues

Subsystems	The Type of Network	
	Closed National Network	Open National Network
3. Blacklisting and content restrictions	• Centralised system • Widespread state censorship and self-censorship • Vigilante groups	• No centralised system • No state censorship, some self-censorship • Little voluntary action
4. Targeted surveillance and data retention	• Widespread and unsupervised • Massive data collection • Localisation of critical data of companies and citizens based on national security	• Restricted and supervised • No massive data retention for security purposes • Data protection and localisation based on privacy issues • Significant portion of critical data abroad
5. Critical information infrastructure	• Owned by the state and private sector • Legal obligation to categorise, maintain and protect • CII mostly state-controlled and duplicated • Ability to disconnect the national network from the global internet	• Owned by the private sector • Protection guided by market economy factors • Some government regulation and certification • No state-level duplication of CII • No ability to disconnect national network
6. Active countermeasures	• State-controlled media • Strict laws to regulate foreign media and foreign ownership of media assets • State-supported religious and patriotic institutions • Dedicated cyber diplomacy organisation with clear national objectives • Overt propaganda, covert and disruptive information operations • Obfuscation of IW capabilities	• State and commercial media • Few restrictions for foreign media companies • Cyber diplomacy part of common foreign policy with diverging interests among allies • Soft power, overt strategic communications and targeted information operations • Official IW forces operating according to law

Subsystems	The Type of Network	
	Closed National Network	Open National Network
7. Management, monitoring, control and feedback	• Multiple centralised information management and incident response systems • Nationally controlled threat response (both technological and psychological) • Directed by the security services • Limited international cooperation and information exchange	• Only a limited national incident response system • Concentrates on cyber crime • National computer incident response team (CSIRT) coordinates and administratively stove-piped CSIRTs execute cyber security • Developing international cyber security cooperation

5. COMPARISON OF ADVANTAGES AND DISADVANTAGES BETWEEN NETWORKS

Kukkola, Ristolainen and Nikkarila (2017) have argued that 'cyber asymmetry' favours a nation closing its networks when the analysis of asymmetry is based on examining attack-vectors. The refining of concepts and the addition of resilience do not significantly change the results of this analysis. Therefore, the analysis below takes prior results as a starting point and adds to them by examining the internal attributes of the networks. The analysis uses the concepts of freedom of action, COP, command and control and resilience to compare open and closed national networks through the seven subsystems of the national system-of-systems of information security and defence. For the sake of clarity, the results are presented from the perspective of the defending nations.

The scientific-technological basis of a closed national network provides a definite advantage in defence through proprietary HW/SW solutions. The basis limits the freedom of action of the attacker who must engage in comprehensive intelligence gathering and reverse engineering. Conversely, the defender knows most of the HW/SW solutions which need to be protected. COP and C2 benefit from domestically produced and integrated systems and cyber resilience is enhanced by a domestically produced and state-controlled ecosystem where observed vulnerabilities can be repaired quickly. The diverse SW/HW solutions of open national networks hinder the freedom of action of the defender. The defender's COP is limited due to legal issues and incompatible technologies while C2 lacks integrated support systems. Resilience is highly dependent on the commercial risk calculations of independent service providers.

The national authentication and encryption system of a closed national network provides a definite advantage in freedom of action and COP to the defender. All traffic is in principle transparent and there are no connections or networks that are closed to the defender. Conversely, the defender of an open national network is limited in its ability to decrypt traffic. The private sector and citizens use solutions closed to the defender. Additionally, domestic encryption solutions are used only in some systems and their quality is mixed although the use of multiple encryption and authentication systems might increase resilience through diversity and redundancy and encryption used in government networks is likely to be tested and certified.

The blacklisting and content restrictions provide a definite advantage for the closed national network defender in freedom of action. Freedom of action of an attacker using information-psychological and technological attacks can be denied by removing resources and platforms from the national cyberspace. Vigilante and similar groups also provide an advantage in COP. A centralised censorship system enhances the speed and effectiveness of C2. The resilience of the whole network is improved as the blacklisting system is tested and operated constantly. Defenders of open networks are disadvantaged in all these categories. They are not impotent, but processes related to blacklisting and restrictions are slow and have legal, political and economic limitations and consequences.

The targeted surveillance and data retention system of a closed national network provides the defender significant advantage in its COP and provides direct access to all public and private networks and their content, thus providing an advantage in freedom of action. As this subsystem is connected to the national centralised management and monitoring systems it also provides an advantage in C2 by providing timely and exact data on cyber and information incidents. The localisation of data to national data centres also enhances resilience. As open national networks officially lack this kind of subsystem they are again disadvantaged. However, once there is enough evidence of a hostile act in the network, open network defenders usually automatically have a mandate to start surveillance and counteractions.

The CII of a closed national network provides the defender advantage in all four categories. The law guarantees freedom of action in private systems and many critical systems are state-owned and controlled. The CII is connected to centralised monitoring and control systems, which gives an advantage in COP and C2. Resilience is high as the CII is constantly monitored, duplicated and protected. The whole national network or parts of it can be disconnected to enable recovery. Although open national network defenders are somewhat disadvantaged, much depends on the policies of those responsible for the CII. Centralised national systems mainly provide COP. Many of the existing systems are administratively stove-piped.

The active information-technological and information-psychological countermeasures provide the closed network defender with a definite ad-

vantage in freedom of action by manipulating information and destabilising opponents. Constant domestic monitoring and foreign espionage operations provide COP, but the advantage in C2 depends on how well actions are coordinated at the state level. Media control and patriotic education provide a definite advantage in information-psychological resilience. The open network defender is somewhat handicapped concerning the overt manipulation of information because of the need to coordinate actions with allies, domestic regulations and international law. This does not, however, mean that it lacks the necessary capabilities when needed. Democracy and transparency might also provide psychological resilience.

The management, monitoring, control and feedback system of a closed national network provides the defender with an advantage in all categories. Interconnected state-controlled systems enable freedom of action and provide national-level COP. The attacker's freedom of action is denied by centrally controlling the structure of the network. Support systems and centralised and hierarchical organisations provide superior C2. Resilience is enhanced as CII is continuously monitored, threats countered and personnel trained. The open national network defender is disadvantaged because of administrative stove piping. The defender might have an advantage in COP through international cooperation and voluntary public-private cooperation but only if the acquired information can be properly collected, analysed and quickly acted upon.

Although this comparison seems to favour closed national networks, this is not necessarily so. Closed national networks are dependent on state participation and, thus, on budgets and administrative efficiency. Domestic encryption solutions and the use of proprietary code do not automatically translate to better security. Politically motivated censorship breeds resistance and disillusionment and, at worst, increases the insider threat. Data retention creates troves of information that can be exploited by foreign hackers. Bureaucratic control of the CII creates overheads, disincentivises innovation and, ironically, produces target lists for the adversary. Authoritarian overtures are hard to mask in cyber diplomacy and create negative feedback from the international community. Citizens recognise propaganda and become disenchanted and passive as a result. Centralised and automated management and control systems are themselves the target of offensive cyber operations and can become victims of bureaucratic infighting and corruption. Despite these reservations, this analysis demonstrates that structural cyber asymmetry is also present when closed and open national networks are analysed based on their internal properties. The addition of resilience as a category of analysis just strengthens the argument.

6. Strategic Implications

The analysis presented in this chapter strengthens the argument that the Russian national segment of the internet, if successfully constructed, will lead to structural cyber asymmetry against nations leaving their networks

open. This asymmetry will provide both defensive and offensive advantage. Thus, the strategic effects of structural cyber asymmetry seem obvious. The mechanisms and consequences of those effects are less obvious. Future developments might also challenge the presumption that any state will risk leaving its networks open. Russia's search for 'asymmetric responses' in the constant great power struggle might accelerate the fracturing of the internet into nationally controlled segments protected by military cyber forces.

Russian national system-of-systems of information security and defence should not be considered only as a 'kill switch'. If successfully deployed, it will be a system-of-systems constructed to control and manage the national information space in a continuum of interstate relations. These relations cover peaceful and intensified competition, conflict, the initial period of war, and war. The system is a response to all kinds of threats from terrorism, internal disturbances, revolutions and regional wars up to a total great power war fought with nuclear weapons. The system enables the flexible adjustment of control of the national information space. The national segment can even fragment along territorial lines into separate and internally functioning parts. A nation that can protect itself or at least ensure the continuity of the nation and state is in the position to perform a pre-emptive or even preventive attack and survive a counterstrike. Moreover, the system enables the creation of power through state-led innovation policies and a centralised management system of the information economy and society. It forms the information-technological basis for winning the constant measure-countermeasure struggle between great powers. The construction of the system in peacetime provides opportunities for exercising its full employment. Consequently, the elimination and mitigation of critical vulnerabilities and interdependencies are possible before a truly closed national network is deployed.

The decision on how to adjust the borders and internal functioning of a national segment of internet is a political question and depends on the perceived threat. The military-strategic implications of national segments are complex. The national segment will probably be disconnected in the case of a nation-wide insurgency or before the initial period of war in a regional or great power war. A flexible increase in control of the information space is enough to counter other kinds of threats. To be militarily effective, the disconnection must be conducted as soon as and as surprisingly as possible. However, economic and political reasons might delay the decision and hastiness could lead to cascading technical failure of the complex system. Outside a conflict situation, the ability to disconnect the national segment can be considered as part of deterrence by denial. The ability to conduct offensive operations from behind the protection of a national segment enables punishment. However, deterrence signalling can be misinterpreted for various reasons. A state closing its networks might be preparing the battlefield and considering a pre-emptive or even preventive attack, instead of just protecting itself from external information and cyber operations. Escalation management and control gains an additional dimension as states begin actively

to manipulate their cyber and information space. Decision-makers might feel themselves secure behind the walls of national segments and engage in brinkmanship. The attacker might more readily use conventional or even nuclear force if cyber means are denied. However, if the defender feels that its strategic C2 systems are secure, it might lessen the pressure to conduct first strikes. Furthermore, national segments might still be reachable through or dependent on foreign assets despite all the efforts to achieve true technological self-sufficiency. It is possible that, if the defender wants to deny the freedom of action of the attacker, it must conduct operations against foreign networks and systems, which might escalate the conflict.

These arguments demonstrate that the panacea of structural cyber asymmetry might have unforeseen consequences, some of which already seem to be emerging. For example, the attributes and capabilities listed in Table I do not reflect the changes in Western policies during 2015–2020. During this period, the 5G and supply-chain security debate has led to the tightening of domestic market regulation. Many states pursue limited domestic HW/SW production and cryptography is increasingly seen as an issue of sovereignty. Military cyber forces are seriously considering 'proactive deterrence' instead of just defending their own networks. National data centres for domestic data and national cyber security centres are being built. Even the principle of territorial cyber sovereignty is being promoted by some Western countries.[8] These policies are a response to the evolving character of cyber conflict and the changing of great power relations. Open networks are becoming less open. From the viewpoint of 2020, it would seem that the asymmetric advantages of closed national networks are diminishing.

The self-evident military response to structural cyber asymmetry is to create one's own closed national network to deter enemy attacks. It is likely that future wars are preceded by prolonged psychological operations to weaken the enemy already in peacetime, and in some cases countries can even achieve the same objectives as they would by launching kinetic attacks simply by delegitimising the regime in the eyes of its citizens through information operations. Disconnecting, or at least efficiently controlling the internet therefore makes sense for any government—authoritarian and democratic alike—in order to deter potential foreign information operations against its population. However, as the analysis of the Russian project presented in this chapter and research on the Chinese policies elsewhere (Inkster, 2016) have shown, a national segment of the internet is inherently an authoritarian project. Disconnecting the national network might not even produce the benefits sought. Moreover, the risks of closing national networks to the national and global information society and economy and the integrity of alliances, such as NATO, are real. Although NATO and its partners must find an answer to 'asymmetric responses', they should not follow the rules set by authoritarian states. Some scholars have proposed that democracies should join their socio-technical-economic systems to secure the existing substrate of cyberspace (Demchak, 2020). Others have argued that malign actors should be

[8] On these developments, see e.g. Tikk & Kerttunen, 2020.

challenged persistently and proactively in cyberspace (Fischerkeller & Harknett, 2019). Still others promote norm-building by the international community to defuse the ongoing cyber arms race (Tikk & Kerttunen, 2020). All these propositions have merit. However, perhaps the most important question is whether Western states should accept the idea of cyber sovereignty, or even information sovereignty. If the concept of sovereignty is adopted then the nature of 'cyber borders', the responsibilities of states concerning those borders and the role of the military in protecting them must be defined soon. The chosen definitions have significant consequences as there is the possibility that in the effort to ensure national security in cyberspace the democratic states and alliances such as NATO and the EU end up hitting the 'kill-switch' on the global internet.

7. REFERENCES

Literature

Ackoff, R.L. (1971) Towards a System of Systems Concepts. *Management Science*. 17 (11), 661–671.

Ajir, M. & Vaillant, B. (2018) Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, 12(3), 70–89.

Blank, S. (2013) Russian Information Warfare as Domestic Counterinsurgency. *America Foreign Policy Interests*. 35 (1), 31-44.

Brantly, A.F. (2016) *The Decision to Attack. Military and Intelligence Cyber Decision-Making*. Athens, Georgia, University of Georgia Press.

Checkland, P. (1993) *Systems thinking, Systems Practice*. New York, John Wiley & Sons ltd.

Chen, J.Q. (2019) A Strategic Decision-Making Framework in Cyberspace. In: Sarfraz, Muhammad (ed.) *Developments in information security and cybernetic wars.* Hershey, PA, IGI Global, 64–75.

Dear, K. (2019) Will Russia Rule the World Through AI? *The RUSI Journal.* 164 (5–6), 36–60.

Demchak, C. (2020) Cybered Conflict, Hybrid War and Informatization Wars. In: Tikk, E. & Kerttunen, M. *Routledge Handbook of International Cybersecurity*. London and New York, Routledge, pp. 36–51.

Drake, W.J., Cerf, V.G. & Kleinwächter, W. (2016) *Future of the internet Initiative White Paper. internet Fragmentation: An Overview.* World Economic Forum, January 2016. Available from: https://www.itu.int/net4/wsis/forum/2016/Agenda/Session/169 [Accessed 9th February 2018].

Elbanna, S. (2006) Strategic decision-making: Process perspectives. *International Journal of Management Reviews*. 8 (1), 1–20.

Endsley, M.R. (2015) Situation Awareness Misconceptions and Misunderstandings. *Journal of Cognitive Engineering and Decision Making*. 9 (1), 4–32.

ENISA. (2015) *Critical Information Infrastructures Protection approaches in EU*, July 2015. Available from: https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf [Accessed 15th September 2020].

Ermoshina, K. & Musiani, F. (2017) Migrating Servers, Elusive Users: Reconfigurations of the Russian internet in the Post-Snowden Era. *Media and Commu-*

nications, 5 (1), 42–53.

European Commission. (2020) *Reports and Studies about Digital Economy and Society Index*. Available from: https://ec.europa.eu/digital-single-market/en/reports-and-studies/76018/3650 [Accessed 14th July 2020].

Fischerkeller, M.P. & Harknett, R.J. (2019) Persistent Engagement, Agreed Competition and Cyberspace Interaction Dynamics and Escalation. *The Cyber Defense Review*. Special Edition International Conference on Cyber Conflict (CYCON U.S.) November 14 -15, 2018, 267-287.

Gartzke, E. (2013) The Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth. *International Security*. 38 (2), 41–73.

Giles, K. (2016) *Handbook of Russian Information Warfare*. Fellowship monograph 9. Rome, NATO Defence College.

Hayes, R.E. & Alberts, D.S. (2005) *Power to the Edge. Command... Control... in the Information Age*. Washington D.C., CCRP.

Hitchens, T. & Goren, N. (2017) *International Cybersecurity Information Sharing Agreements*. Center for International & Security Studies. Maryland, University of Maryland.

Hoffman, D.E. (2009) *The Dead Hand. The Untold Story of the Cold War Arms Race and Its Dangerous Legacy*. New York, Anchor Books.

Howard, R. & Abbas, A.E. (2015) *Foundations of Decision Analysis*. London, Pearson.

Humbert, C. & Joseph, J. (2019) Introduction: the politics of resilience: problematising current approaches. *Resilience*. 7 (3), 215–223.

Inkster, N. (2016) *China's Cyber Power*. New York, Routledge.

International Telecommunication Union (ITU). (2015) *Global Cybersecurity Index & Cyberwellness Profiles, April 2015*. Available from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf [Accessed 15th September 2020].

Jonsson, Oscar. (2019) *The Russian Understanding of War: Blurring the Lines between War and Peace*. Washington, D.C., Georgetown University Press.

JP 3-13. (2014) Joint Chiefs of Staff. *Joint Publication 3-13, 27 November 2012 Incorporating Change 1 20 November 2014*. Available from: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf [Accessed 14th September 2020].

Kallberg, J. & Cook, T. S. (2017) The Unfitness of Traditional Military Thinking in Cyber. Four Cyber Tenets That Undermine Conventional Strategies. *IEEE Access*. 5, 8126–8130.

Kari, M. J. (2019) *Russian Strategic Culture in Cyberspace Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats*. JYU Dissertations 122. Jyväskylä, Jyväskylän yliopisto.

Kiviharju, M., Huttunen, M. & Kantola, H. (2020) Finnish View on the Combat Functions in the Cyber Domain. In: Eze, T., Speakman, L. & Onwubiko, C. (Eds.) *Proceedings of the 19th European Conference on Cyber Warfare and Security. A Virtual Conference hosted by University of Chester UK* 25-26 June 2020, pp. 186–194.

Kukkola, J. (2020) *Digital Soviet Union. The Russian national segment of the internet as a closed national network shaped by strategic cultural ideas*. National Defence University Series 1: Research Publications No. 40. Helsinki, National Defence University.

Kukkola, J., Ristolainen, M. & Nikkarila, J-P. (2017) *Game Changer: Structural Transformation of Cyberspace*. Finnish Defence Research Agency Publications 10. Riihimäki, Finnish Defence Research Agency.

Kukkola, J., Ristolainen, M. & Nikkarila, J-P. (2019) *Game Player. Facing the structural transformation of cyberspace*. Finnish Defence Research Agency Publications 11. Riihimäki, Finnish Defence Research Agency.

Kuusisto, R., Kuusisto, T., & Armistead, L. (2005) Common Operational Picture, Situation Awareness and Information Operations. In: Hutchinson, B. *Proceedings of the 4th European Conference on Information Warfare and Security*. Glamorgan, UK, 2005, pp. 175–185.

Latukhina, K. (2018) The President urged to work together to fight the cyber threat to protect digitalisation. *Rossiiskaia Gazeta*, 8.7.2018. Available from: https://rg.ru/2018/07/08/putin-nazval-borbu-s-kiberatakami-gosudarstvennoj-zadachej.html [Accessed 18 September 2020].

Libicki, M.C. (2016) *Cyberspace in Peace and War*. Annapolis, Maryland, Naval Institute Press.

Liff, A. (2012) Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*. 35 (3), 401–428.

Multinational Experiment 7 (MNE7). (2013) *Outcome 3 Cyber Domain Final Report February 2013. Cyber Situational Awareness Standard Operating Procedure.* Available from: https://www.hsdl.org/?view&did=760553 [Accessed 31st July 2020].

NATO. (2016) *Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organisation, 16th December 2016*. Available from: https://www.nato.int/cps/en/natohq/official_texts_138829.htm [Accessed 15th September 2020].

NATO. (2020) *Allied Joint Doctrine for Cyberspace Operations, AJP-3.20, Edition A Version 1, January 2020*. NATO Standardization Office (NSO), 2020. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf [Accessed 13th July 2020].

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). (2020) *Strategy and Governance*. Available from: https://ccdcoe.org/library/strategy-and-governance/ [Accessed 14th July 2020].

Nocetti, J. (2018) Cyber Power. In: Tsygankov A.P. *Routledge Handbook of Russian Foreign Policy*. London and New York, Routledge, 2018, pp. 182–198.

Nye, J.S. Jr. (2017) Deterrence and Dissuasion in Cyberspace. *International Security*, 41 (3), 44–71.

O'Brien, J. A. & Marakas, G. M. (2011) *Management Information Systems (10th edition)*. New York, NY, McGraw-Hill, Irwin.

Pynnöniemi, K. (2018) Russia's National Security Strategy: Analysis of Conceptual Evolution. *The Journal of Slavic Military Studies*, 31 (2), 240–256.

Rid, T. & Buchanan, B. (2015) Attributing Cyber Attacks. *The Journal of Strategic Studies*. 38(1-2), 4–37.

Ristolainen, M. & Kukkola, J. (2019) Closed, safe and secure – the Russian sense of information security. In: Benson, Vladlena & McAlaney, John (Eds.) *Emerging Cyber Threats and Cognitive Vulnerabilities*. London, Academic Press, pp. 53–71.

Ross, R., Graubart, R., Bodeau, D. & Mcquaid, R. (2018) Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. *Draft NIST Special Publication 800-160 Volume 2, 2018*. Available from: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf [Accessed 1st May 2020].

Simon, H. (1997) *The New Science of Management Decision*. Englewood Cliffs, NJ, Prentice Hall.

Shanghai Cooperation Organisation (SCO). (2009) *Agreement between the governments of the member states of the Shanghai Cooperation Organisation on cooperation in the field of ensuring international information security, 16th June 2009, Ekaterinburg*. Available from: https://base.garant.ru/2571379/ [Accessed 29th March 2019].

Sheremet, I. A. (2019) Ensuring cybersecurity in the context of the development of the digital economy [In Russian]. *The Bulletin of the Moscow University*. Series 25: International relations and world politics, 11 (1), 3–9.

Soldatov A. (2017) The Taming of the Internet. *Russian Social Science Review*, 58 (1), 33–39.

Thomas, T.L. (1998) Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations. *The Journal of Slavic Military Studies*, 11 (1), 40–62.

Thomas, T. (2017) *Kremlin Kontrol: Russia's Political-Military Reality*. Fort Leavenworth, KS, FMSO.

Thornton, R. & Miron, M. (2020) Towards the 'Third Revolution in Military Affairs'. *The RUSI Journal*, 165 (3), 12–21.

Thurner, S., Hanel, R. & Klimek, P. (2018) *Introduction to the Theory of Complex Systems*. Oxford, Oxford University Press.

Tikk, E. & Kerttunen, M. (Eds.) (2020) *Routledge Handbook of International Cybersecurity*. London and New York, Routledge.

Vendil-Pallin, Carolina. (2017) Internet control through ownership: the case of Russia. *Post-Soviet Affairs*, 33 (1), 16–33.

Legislation

FZ-126. (2003) Federal law 07.07.2003 No 126-F3 (updated 07.04.2020) *'On Communications'* [In Russian]. Available from: http://www.consultant.ru/document/cons_doc_LAW_43224/ [Accessed 18th September 2020].

FZ-90. (2019) Federal law 01.05.2019 No 90-FZ *'On the changes to the Federal law on communications and the Federal law on information, information technology and information security'* [In Russian]. Available from: http://www.consultant.ru/document/cons_doc_LAW_323815/ [Accessed 8th May 2020].

RP-788. (2015) Degree of the Government of the RF 30.4.2015 N 788-p *'On the signing of an Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of ensuring international information security'* [In Russian]. Available from: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=620700#04623583645026 8 [Accessed 18th September 2020].

RP-1632. (2017) Degree of the Government of the RF 28.07.2017 N 1632-r *'On the approval of the program 'Digital Economy of the Russian Federation'* [In Russian]. Available from: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf [Accessed 23rd January 2018].

Ukaz-646. (2016) Order of the President of the RF 5.12.2016 N 646 *'On the approval of*

the doctrine of information security of the Russian Federation' [In Russian]. Available from: http://rulaws.ru/president/Ukaz-Prezidenta-RF-ot-05.12.2016-N-646/ [Accessed 21st March 2019].

Ukaz-203. (2017) Order of the President of the RF 09.05.2017 No 203 *'On the Strategy of the development of information society in the Russian Federation in the period 2017-2030'.* Available from: https://www.garant.ru/products/ipo/prime/doc/71570570/ [Accessed 18thth September 2020].

Ukaz-474 (2020) Order of the President of the RF 21.7.2020 N 474 *'On the national goals of development of the Russian Federation in the period to 2030'* [In Russian]. Available from: http://publication.pravo.gov.ru/Document/View/0001202007210012 [Accessed 1st November 2020].

Russia's Cyber Limitations in Personnel Recruitment and Innovation, Their Potential Impact on Future Operations and How NATO and Its Members Can Respond

Joe Cheravitch
Doctoral Student
King's College London

Bilyana Lilly
Policy Researcher
Frederick S. Pardee RAND Graduate School
RAND Corporation

Abstract: While Moscow's willingness to launch cyber operations depends in no small part on how the Russian leadership interprets geopolitics, resources and personnel determine the ability to conduct them. Russia has demonstrated a capacity to craft sophisticated malware to support operations that range from espionage to disrupting critical infrastructure, to interfering in states' internal affairs through cyber-enabled influence campaigns, but the government still faces difficulties recruiting and retaining the needed technological talent to keep pace with its rivals. While some of the factors inhibiting the growth of Moscow's cyber programme are internal to the organisations tasked with executing them, such as a culture-clash between specialist recruits and the bureaucracy, the most significant impediments are exogenous to them and include brain-drain and the health of Russia's economy. Moscow's litany of perceived adversaries in cyberspace ensures continuous efforts by the state to prevent the emigration of computer science and IT specialists and expand the ranks of those serving Russia's offensive and defensive cyber capabilities. As evolving technologies like artificial intelligence and quantum computing carry implications for future cyber operations, Moscow's ability to marshal its resources to remain competitive in a furtive digital arms race similarly depends on many of these factors.

This chapter aims to address key questions arising from the probable gap that separates Russian cyber personnel and capabilities, especially technological innovation, from its ambitions and what effect this disparity might have on future state-backed cyber campaigns. It starts by accounting for different factors that affect the ability of Russia's military and security services to successfully expand recruiting and support technological innovation related to cyber operations. This is followed by an examination of various initiatives and strategies that Russian agencies have introduced to address Russia's cyber limitations and cultivate technological innovation. Finally,

it discusses how Russia's current official policies and informal practices are likely to affect the nature of its cyber operations in the future and to what extent NATO and its members can leverage these limitations to achieve desired effects in the Alliance's cyber security efforts.

Keywords: *Cyber, multi-domain, cross-domain, concepts, Russia, China*

1. INTRODUCTION

As states seek to build a capacity to defend against cyber operations and, to varying extents, conduct their own, virtually all face considerable hurdles when staffing and resourcing their cyber forces.[1] In many cases, the challenges are universal: disproportionate salaries and benefits between public organisations and private enterprise, or vast cultural differences between government and private employment that typically pushes freethinking and autonomous programmers toward the private sector. States are forced to cultivate offensive and defensive capabilities within the confines of budgets and personnel quotas amidst an ever-changing and largely unpredictable operational environment. While pooling resources among allies could improve their ability to better manage these developments, such opportunities are few as the sheer level of trust needed to share effective and unattributable malware or aspects of cyber security surrounding critical infrastructure drives partners to err on the side of classification. Some of the challenges in developing proprietary capabilities are distinct to certain governments with aspirations to compete in this space. For instance, countries peripheral to global technological innovation that nonetheless hope to protect national networks, if not exploit those of their adversaries, must consistently access technology and components developed beyond their borders. Cyber and traditional espionage provide at least an intermittent avenue to acquire an adversary's capabilities, though access can end abruptly and the discovery of these efforts may beget a response. Some countries including Russia and China must reconcile the operational boon provided by incorporating criminal elements into the state's agenda while ensuring these partnerships keep contracted, co-opted or coerced hackers from targeting the same networks the government seeks to defend, usually through tacit arrangements that promise incarceration for doing so while tolerating criminals' unsanctioned operations against external targets (Maurer, 2018; Marks, 2020).

Moscow has faced a plethora of challenges in building the kind of offensive and defensive cyber capability deemed necessary to thwart and reciprocate perceived activity from Russia's rivals, chiefly NATO member states. Some of these obstacles are among the seemingly universal ones mentioned earlier, while others are distinct. Probably foremost among them is the persistent

[1] For instance, the US military's Cyber Command (CYBERCOM) as of late 2018 faced recruiting challenges despite enhanced recruiting measures and a larger budget. A particular lack of 'coders' and 'developers' stunted the growth of CYBERCOM's Cyber Mission Force at the time, while a US defence department report found that existing specialists lacked the necessary experience to make a 'credible strategic cyber capability' (Pomerleau, 2018).

emigration of technological expertise from Russia, a trend that has existed in ebbs and flows since the collapse of the Soviet Union. Other factors exogenous to Russia's national security structure such as the state of Russia's economy and the ongoing global Covid-19 pandemic likely intermittently serve as a brake on developing the technology and personnel needed to compete with peers and adversaries in cyberspace, at least in absolute terms. The Russian government has addressed these challenges by creating a dedicated cyber force and using the support of a variety of non-governmental actors and agencies. The government has also established institutions and initiatives aimed to stimulate technological innovation. Despite its efforts, these limitations continue to shape how Moscow pursues the development of its cyber capabilities and the strategy guiding their use, suggesting that analysis of these trends, including state efforts to circumvent or alleviate them, would help to discern future Russian cyber operations, most importantly the campaigns targeting everything from Western elections to global critical infrastructure.

Research for this paper includes a mix of scholarly, journalistic and non-traditional sources that collectively offer valuable open source insights into Moscow's cyber limitations and how they might affect future activity. It concentrates on Russian state organisations, primarily the military and intelligence services and their connections to Russian academia, the IT industry, criminal hackers and other third parties. The opacity surrounding Russian and other states' cyber capabilities, however, affords the analysis and judgments in this paper a moderate level of confidence, as operational security prevents the fidelity needed to definitively assess the strengths and weaknesses facing relevant programmes.

2. Factors Limiting the Growth of Russia's Cyber Programmes

Russia can count on few if any allies in terms of cyber operations that have increasingly supported Russian foreign policy and military objectives that stretch from Syria to the US. The resources Moscow can allocate to cyber programmes are almost certainly eclipsed by those available to its principal rival in cyberspace, the NATO Alliance.[2] Despite ongoing debates about the actual size of Russia's defence budget, NATO military spending—even excluding the US—exceeds Russia's several times over (Wezeman, 2020), though unclassified budgetary comparisons fail to account for clandestine expenditures under which most states almost certainly place their offen-

[2] Although there are extremely few public cases of states cooperating in offensive cyber operations, at least some evidence suggests Russia's chief rivals have done so. The US, for example, allegedly collaborated with Israel in creating the Stuxnet virus that targeted Iran's nascent nuclear programme (Nakashima and Warrick, 2012). Additionally, NATO members in late 2017 agreed on a more aggressive approach to Russian cyber aggression that reportedly included offensive activity, according to a former NATO official, though the level to which offensive capabilities were actually shared or integrated into the Alliance structure remains unclear (Ali, 2017).

sive cyber efforts. In response to US plans in early 2015 to increase spending on cyber, including almost $17 billion partly dedicated to boosting US Cyber Command's capabilities,[3] Moscow reportedly mustered as much as $250 million, part of which was dedicated to offensive capabilities (Gerden, 2016). A 2017 assessment published by a Russian IT firm that ranked states' cyber capabilities, which included 'espionage, offensive cyber operations and information warfare' ranked Russia fifth in global 'cyber power', with roughly less than five per cent of the budget for cyber programmes as the US supposedly had and slightly over ten per cent of its reported manpower (Korotaev, 2017). Granted, the kind of cyber operations long conducted by Russian state actors, one of the cost-effective means of asymmetrically outflanking quantitatively superior adversaries prescribed by Putin in 2006,[4] almost certainly require a fraction of the spending on cyber made by Moscow's rivals, at least while at peace. Larger ambitions, however, such as establishing cyber capabilities and forces that move closer to parity with Russia's perceived adversaries, or initiatives to reduce software and hardware import dependencies on many of those same states, require a higher level of resourcing. Keeping pace with these rivals as emerging technologies such as quantum computing play a larger role in future cyber operations similarly necessitates increased funding and personnel.

A drought in state resources following the collapse of the Soviet Union all but crippled Moscow's nascent efforts to keep pace with observed Western developments in cyber capabilities. Sergey Aleksandrovich Modestov, a current vice-president of the Russian Academy of Military Science, claimed in 1997 that the 'widespread opinion' that Russia lagged the West in computing technology by as much as a decade necessitated a redoubling of Moscow's efforts to 'control and create a new class of weapons' (Modestov, 1997). Even as Russia underwent fiscal and economic stabilisation and as Russian society increasingly accessed the internet at exponential rates, Moscow struggled to connect advances in computer science and information technology to state goals surrounding national security, in part because of distinct cultural and bureaucratic impediments to government innovation. A 2005 RAND report found that a 'cult of secrecy' inhibited Moscow's efforts to integrate information technology into state functions including national security as state entities often used 'privileged information' to boost their interests at the

[3] According to official sources, the US intelligence community's Military Intelligence Programme (MIP) budget for fiscal year 2015 amounted to $16.6 billion (ODNI, 2020). The Deputy Director of the National Security Agency testified to the US House of Representatives Armed Services Subcommittee on Intelligence, Emerging Threats, and Capabilities and claimed that the MIP in 2015 would 'focus on the development of a strong cyber workforce and intelligence gathering in cyberspace' focused on US Cyber Command (US Government Publishing Office, 2014).

[4] Putin in 2006 in an address to Russia's federal assembly stated: "We must take into account the plans and directions of development of the armed forces in other countries; we must know about perspective developments. But do not chase quantitative indicators, do not 'burn' money in vain. Our answers must be founded on intellectual superiority. They will be asymmetric, less expensive." (Kremlin.ru, 2006).

expense of one another, a practice exacerbated by President Putin's placing intelligence officers in prominent positions (Peterson, 2005). While Moscow has since adopted measures to mitigate some of these problems, with mixed success, several shortcomings continue to hold back the state's effort to bolster its cyber capabilities.

The most significant impediment is likely the consistent 'brain drain', the emigration of IT and computer science specialists from Russia to other countries, especially the West. Nataliya Kasperskaya, chair of the board of the association 'Fatherland Soft' (*Otechestvenniy soft*) and ex-wife of renowned Russian cyber security mogul Eugene Kaspersky, recently submitted a letter to Prime Minister Mikhail Mishustin warning that Russia could lose between 10 to 15 thousand IT specialists in the next year (Skobolev, 2020). But dissatisfaction with salaries is longstanding; in 2017, a survey by Russoft found that Russian programmers were unhappy with their pay even as wages rebounded from their precipitous decline between 2014 and 2016 (Russoft, 2017a). According to a 2019 survey conducted by the Atlantic Council, IT specialists and software engineers comprised the third-most prominent category of Russian professionals choosing to live and work in other countries (Herbst and Erofeev, 2019). The effects on Russia's IT and computing industries by the coronavirus pandemic exaggerate an already dire trend for Moscow regarding the flight of technological specialists. Comparing May this year and the same period in 2019, Russian software developers' average revenue fell by almost half and ten per cent of firms claimed earnings declined by more than 90 per cent (Kozlov, 2020).

Prime Minister Dmitriy Medvedev in 2017 and Deputy Prime Minister Dmitriy Rogozin in 2018, described brain drain as a significant problem for Russia's development and future competitiveness (RBC.ru, 2017; 2018). The low salaries for specialists in Russia compared to those offered in the West, plus the internationally recognisable quality of Russia's leading scientific academic institutions, create an outward flow of specialists. In 2018, another survey revealed that as much as 65 per cent of Russian IT specialists planned to work abroad for higher salaries, though most surveyed stated they would eventually return to Russia after gaining 'international experience' (Romanova, 2018). As the military strove to build an 'information operations force' and as Rostec expended more funds on securing Russia's critical networks, the dearth of specialists became apparent as mounting evidence showed their preference to leave Russia for the West (Khodarenok and Zatari, 2017). Moreover, the interference of the state in private enterprise has contributed to the departure of specialists, including the IT sector. Pavel Durov, the founder of Russia's foremost social media platform 'VKontakte', left Russia in mid-2017 at least ostensibly because of demands from Russia's Federal Security Service (FSB) to provide information on his platform's users (Heller, 2018). The departures of key figures like Durov have a disproportionate impact on Russia's IT industry. As Russoft described in its 2019 survey of Russia's IT industry, 'even the loss of one key employee who is leaving the country is a problem for a specific company, particularly when this person is the most

competent developer who knows foreign languages' (Russoft, 2019: p. 144).

Whatever Moscow's personnel and resource limitations, Russia's hackers have given little sign that these shortcomings affect operations, at least during peacetime, which have ranged from attacking the 2018 Winter Olympic Games to probing electric grids in the US.[5] Nevertheless, in an unlikely scenario involving impending overt conflict between Russia and NATO, the limitations facing the former would probably affect its ability to conduct concurrent and sustained efforts against at least a quantitatively superior foe. When Russian state-sponsored actors launched waves of fairly simple yet massive distributed denial of service (DDoS) attacks against largely unprepared networks in Estonia in 2007 and Georgia in 2008, Western intelligence services and allies purportedly developed malware unparalleled in its sophistication and purpose: the Stuxnet malware used to temporarily disrupt Iran's nuclear programme required the work of multiple teams for development and extensive facilities for testing (Zetter, 2014). While DDoS served Moscow's purposes at the time and as it continues to occupy a prominent spot in state and non-state cyber arsenals, the examples of Stuxnet and the Estonia and Georgia cases to some extent highlight the probable gulf in capabilities between Russia and the West at the time.[6] Time also probably influenced these operations: while Stuxnet is described as being planned and developed years in advance of its use, Russian operators tasked with attacking Estonian and Georgian networks had far less lead time to prepare offensive cyber operations, given the comparative abruptness of the events that precipitated the 'bronze soldier' incident in Estonia and the war with Georgia a year later. The earliest available samples of the 'Regin' malware, considered by cyber security experts as the most advanced malware ever created and reportedly the work of the US's National Security Agency (NSA), date from 2011 (Cimpanu, 2019), a time when Russian military intelligence (GRU) officers resorted to spontaneously contacting cyber security researchers to hand over exploits (Satter and Bodner, 2018). Undoubtedly, Russian

[5] While much has been written about the blurring of peace and war from the Russian military perspective, several Russian military authors nonetheless distinguish between peace and theoretical wartime cyber operations. These authors typically distinguish between the types of operations that shape peacetime cyber, or 'information confrontation' efforts, like cyber efforts directed at strategic deterrence and wartime cyber operations, which generally aim to achieve information predominance over the enemy and aid kinetic military operations (Sayfetdinov, 2014; Lata, Annenkov and Moiseev, 2019; Dylevskiy, Komov and Petrunin, 2013).

[6] The gap in cyber espionage capabilities between Russia and its rivals at the time, however, was likely narrower than that separating offensive cyber operations. For instance, malware components that constituted what would eventually become APT28, attributed to Russia's GRU, date back to 2004 and continuously evolved alongside successful hacks against a wide array of targets (FireEye, 2014). Similarly, Turla, a threat group attributed to Russia's Federal Security Service (FSB), predates APT28 and has consistently impressed cyber security researchers through sophisticated breaches of targeted networks, including the 'agent.btz' exploitation of classified US military networks in 2008 (Council on Foreign Relations, 2020).

cyber capabilities drastically improved between then and the more notable and recent operations following Russia's annexation of Crimea in 2014. But some of these successes were predicated on malware likely developed by its rivals, such as the repurposing of alleged NSA intrusion sets for the 'BadRabbit' ransomware and 'NotPetya' wiperware attacks in 2017 (Stubbs, 2017), suggesting Russian malware development continued to lag behind that of its foremost adversaries. These capabilities are certainly enough to match Moscow's goals of engaging in information warfare along various fronts during uncertain peace and Russian actors have even recently demonstrated the ability to create original tools to advance these campaigns.[7] But to lead the international community in emerging technologies relevant to cyber capabilities, as prescribed by Putin in 2017, Russia needs more than current limitations allow.

Perhaps one of the most salient technological pursuits for offensive cyber operations is quantum computing, particularly its application to decrypting digital codes used by an adversary. As described by US Army Cyber Institute researchers in 2020, an adversary could use this technology to 'efficiently break the universally adopted public-key cryptographic schemes' in place today (Beshaj and Hall, 2020: p. 351). While Moscow hopes to develop unique capabilities in this field, including an ongoing effort by the Foundation for Advanced Research Projects (TASS, 2020), it continues to lag far behind leaders in the field, chiefly the intense competition internal to the US private sector. Additionally, artificial intelligence promises to advance both defensive and offensive capabilities, such as automatic defensive systems capable of formulating and deploying patches or social media automated phishing and reconnaissance on the offensive side of operations (Howells and Kalfoglou, 2020). Experts, however, describe Russia as a laggard in this field as Nikolai Markotkin of the Russian International Affairs Council and Elena Chenenko of Kommersant claimed in August 2020:

> Even if artificial intelligence (AI) development becomes Russia's highest priority, Moscow has no chance of catching up with Washington and Beijing in this field. Under favourable conditions, however, it is quite capable of becoming a serious player and even a local leader in certain areas (Markotkin and Chernenko, 2020).

These developments in Russia occur against a backdrop of serious deficiencies in national cyber security. While Moscow has demonstrated a clear and consistent interest in improving this, efforts to boost critical infrastructure cyber security are under-resourced and mired in stalled initiatives to reduce dependence on foreign software and hardware. The extensive use of pirated software to shore up cyber security and an ageing computing infrastructure

[7] For instance, the US National Security Agency and Federal Bureau of Investigation in August 2020 released a report detailing malware used by the GRU's 85th Main Special Service Center (GTsSS), the GRU's leading cyber espionage unit, called 'Drovorub' that deployed 'previously undisclosed' malware to target Linux systems (NSA/FBI, 2020).

also hinder the state's drive to improve these capabilities (Kottasova, 2017). The WannaCry ransomware attack in 2017 affected Russian networks more than those of any other state, extending even to its central bank (Reuters, 2017) as the attack offered a fleeting glimpse into a woefully unprepared cyber security sector.

3.RUSSIA'S INITIATIVES TO ADDRESS ITS CYBER LIMITATIONS

Emerging technologies relevant to cyber capabilities require intensive research and a given state's ability to harness various private and public entities to support these developments is perhaps not as far removed from arms-races of the previous century. That capacity hinges on the state's ability to marshal personnel and resources through collaboration, expropriation, coercion or otherwise to meet research goals. While Moscow has been able to seemingly keep its adversaries on the back foot in recent years through brazen offensive cyber operations and a distinct ability to merge hacks with digital psychological operations, its ability to remain competitive as communications and computing technologies become more sophisticated is less clear.

To manage or mitigate its shortage of talent, the Russian government has adopted various formal and informal methods. These include: 1) soliciting or coercing individuals and organisations to conduct operations on Moscow's behalf; 2) cultivating technical innovation relevant to state cyber capabilities; 3) expanding direct recruiting programmes; 4) bureaucratic deconfliction; 5) espionage targeting other states' cyber capabilities; and 6) concentrating on 'information-psychological' effects.

A. Soliciting/Coercing Civilian IT Experts and Organisations

The Russian services have a long history of co-opting a variety of cyber experts including criminals and IT specialists from the private sector or 'patriotic' hackers to collaborate with the government in various operations (Maurer and Hinck, 2018; Turovskiy, 2019). As early as the 1980s, Soviet intelligence services made use of an independent German hacker, Peter Karl, who offered to steal secret documents containing technology blueprints for the USSR that could enable the latter to 'overtake the West' (Turovskiy, 2019: p. 125). Today, the relationship with criminal hackers residing in the former Soviet states is based on the tacit agreement that they can conduct their activities unprosecuted by the state as long as they do not target any .ru websites and assist when called to engage in an operation 'for patriotic purposes' (Turovskiy, 2019: p. 148; Maurer and Hinck, 2018). In describing Moscow's control over non-state cyber groups, Russian expert Anton Nosik asserted: 'Each [Russian] hacker, who is not in prison, has a curator. Either in FSB or in Directorate 'K' of Russia's Ministry of Internal Affairs' (Lysenko and Brooks, 2018:p. 4). Such partnerships can help to fill any gaps by developing relation-

ships with independent hackers, some of whom eventually don a uniform.[8]

Even Russia's military, which probably represents the most rigidly hierarchical and subordinated offensive Russian cyber actor, at least occasionally elicits support from independent sources. Alexandra Elbakyan, a programmer from Kazakhstan who founded a website that has leaked thousands of proprietary academic publications, reportedly works occasionally on behalf of Russian military intelligence (Harris and Barrett, 2019).

Russia's intelligence and security services will almost certainly continue to pursue relationships with independent organisations and specialists to boost its cyber capabilities beyond those provided solely by uniformed and official staff. This tactic afforded Moscow a cyber capability even during its post-Soviet nadir in the 1990s when state-backed hackers successfully compromised several US government networks belonging to the military, National Air and Space Administration (NASA), Department of Energy and others (Greenberg, 2019). Incorporating independent sources into these operations received the highest possible endorsement in 2017 when Putin compared patriotic hackers to independent 'artists' acting in the state's interests, though supposedly without its direct backing (RFE/RL, 2017). Given the reliability of independent sources to supplement state-sanctioned cyber operations, the veneer of plausible deniability they afford Moscow and the international community's struggle to address it, their use could even expand in a future in which the gap in cyber capabilities between Russia's official actors and its adversaries widens. Nonetheless, the case of 'Vyarya', a pseudonymous programmer who left Russia after threats from probable security services after he refused to cooperate in offensive cyber research, illustrates that an even heavier hand in soliciting external support can potentially accelerate the flight of qualified specialists (Kramer, 2016). Developing the technologies likely to drive future cyber operations, however, falls outside the purview of independent hackers. Adapting to this future necessitates robust links to an IT sector capable of intensive research and optimising work with state-funding that is a fraction of the resources put forth by Russia's perceived adversaries.

B. Efforts to Cultivate Technical Innovation

Moscow needs a vibrant IT sector to compete with its adversaries and rivals if it hopes to remain at the cutting edge of offensive and defensive cyber capabilities, especially in the unlikely—yet conceivable—scenario in which Russia needs sustained operations against a sophisticated opponent. Russia

[8] The case of Dmitriy Dokuchaev, a renowned Russian hacker gradually integrated into one of the FSB's offensive cyber departments, exemplifies the path from independent hacking to direct state subordination and employment. (Kramer 2017; Turovskiy 2019: p. 139) Dokuchaev, an independent hacker in the mid-2000s, was coopted into working for the FSB's Center for Information Security and eventually became a major in that unit. Similarly, Maksim Yakubets, the leader of a prominent criminal hacking group, in 2017 began working closely for the FSB and – as of early 2018 – awaited a license to work with classified information from the former, though whether Yakubets received a rank and official position within the FSB remains unclear (US Department of the Treasury, 2019).

lacks an equivalent to the Silicon or Shenzhen Valleys and state-directed efforts to cultivate an analogue in Russia have met with, at best, mixed results. Medvedev in 2010 inaugurated an effort to build 'Skolkovo Valley', which he described as 'something along the lines of Silicon Valley' and which by 2020 would host as many as 50,000 specialists (Appell, 2015). The initiative rapidly fell victim to rampant corruption and eventually led Russian officials to re-evaluate its potential. For instance, Viktor Vekselberg, the chairman of the Skolkovo Board of Directors, claimed in June this year that 'Skolkovo is not a counterpart of the Silicon Valley' and comparing them was 'inappropriate and even absurd' (TASS, 2020).

Skolkovo's fate demonstrates that trends in emigration and limited resources are worsened by prevailing corruption, which almost certainly limits Moscow's ability to optimise research and development for projects relevant to cyber capabilities. For example, a military officer who headed a department in the 18th Central Scientific Research Institute (TsNII), which, according to the Russian press, develops 'special radio-electronic technology' on behalf of the GRU, was stripped of his rank and sentenced to six years in prison in 2017 for stealing equipment worth 40 million roubles (Lenta.ru, 2017).[9] That same year, the head of the FSB's Information Security Centre resigned as FSB sources claimed his dismissal due to corruption charges was imminent (Kolomychenko, 2017), though his ouster could have at least partly been political.

Russia's military and security services use the Russian Foundation for Advanced Research (Fond Perspektivykh Issledovaniy, FPI), known as Russia's equivalent to the US Defence Advanced Research Projects Agency (DARPA), to stimulate innovative research and projects that can enhance Russia's cyber capabilities. FPI conducts regular nationwide competitions for innovative technological solutions to national security problems (Moscow Times, 2015) and cyber warfare which as of 2018 constituted one of the three main foci of FPI's research (Uppal, 2019). The winning projects may receive funding to build a prototype of their research and their solutions can then be implemented in the respective agencies of the Defence Ministry (International Military-Technical Forum 'Army-2018', 2018). In 2019, FPI together with Skolkovo Security Challenge launched a competition for the best solution for the 'preventive detection of network attacks.' The participants who won the contest applied machine learning methods to effectively identify 'complex patterns and network anomalies' (FPI, 2019a). The interest of the security services in the ideas developed in these competitions is suggested by the fact that one of the judges of the competition was A. V. Korolkov, chairman of

[9] The 18th Central Scientific Research Institute, or Unit 11135, to some extent likely conducts cyber research. For instance, the unit hosted an unspecified scientific conference in 1995 that helped research related to 'raising the effectiveness of automated operational control systems from the impact of malicious software' (Vyalykh, 1999). The 18th also benefitted from research in 2004 for a contract related to 'Research and development of mathematical and software tools for effective parallelisation of applied problems on high-performance computing systems' (Levin, 2004).

Unit 43753 (FPI, 2019b), the FSB's Communications Security Centre, part of the Eighth Service Directorate (Villalon, 2016).

Nonetheless, the flight of specialists from Russia continues to threaten the overall health of Russia's IT sector and ultimately state actors' ability to tap into it to further their goals related to developing offensive and defensive cyber capabilities. The continued effect of the coronavirus pandemic on Russia's economy has exacerbated the issues driving emigration, suggesting a prolonged effect on the IT sector. Other issues, such as Russia's impending adoption of a law that requires digital assets be purchased in Russia and declared by whoever buys them are likely to spur more emigration. As the head of Russia's cryptocurrency and blockchain associated stated, 'The adoption of the digital financial asset law in its current state is likely to speed up an exodus of IT professionals' (Kozlov, 2020).

C. Expanding Direct Recruiting Programmes

While the Soviet military and intelligence services enjoyed a direct pipeline to highly qualified graduates of technical institutions, these services' post-Soviet descendants must compete with the allure of the private sector when recruiting computer science and IT specialists in modern Russia. Despite the shock of the Soviet collapse, many of the institutions used to train intelligence and military specialists in cyber operations survived into the 21st century, though many initiatives are new. Russia's military, for example, has launched several such efforts since 2013 ranging from 'military science units' to cyber security education programmes at specific universities and schools; for example, the St. Petersburg-based Military Academy of Communications in 2015 launched a cyber security training programme that offered classes on network technology, multimedia hardware, software and robotics (Bodner, 2015). At least some of these programmes seek to inculcate a culture of patriotism among prospective recruits, galvanising them against supposed information and cyber threats emanating from states hostile to Russia. The GRU, for instance, has sponsored 'cadet classes' that provided extra computer lessons alongside patriotic education (Troianovsky and Nakashima, 2018). Another tactic involves direct partnerships with academic institutions or training programmes, sometimes by placing officials connected to Russia's military or intelligence services into positions of leadership. For instance, the former chief of the Federal Agency of Government Communications and Information (FAPSI) and current Director of the National Association for International Information Security, Vladislav Sherstyuk, also serves as the Director of the Institute for Information Security at Moscow State University (NAIIS, 2020).

Since the creation of the military science units, the military has been soliciting applications for mathematicians, cryptographers, engineers and programmers among technical universities (Turovskiy, 2019). President Putin's 2018 visit to the 'ERA' (Elite of the Russian Army) Technopolis, which is partly based on that recruiting initiative, exemplified the importance of harnessing Russia's technical talent for defence research (Shurygin, 2018) and

he also inspected the ERA's work at the 'Army 2019' exposition near Moscow that year (Vesti, 2019). Although those entering the science companies are only obligated to serve a year of military service, the standard conscription term for Russia's military, they are encouraged to become officers after their mandatory service (Lysenko and Brooks, 2018).

According to Turovskiy (2019), since 1991 the FSB has been conducting Olympiads on cryptography in Russian schools. The services have continued to use various practices to seek young hackers. In 2015, a course titled 'Young programmers of Russia's FSB' appeared in a Moscow-based academy for children in secondary education, which prepared students to become IT experts and taught them how to launch DDoS attacks and exploit wireless networks, all while attending meetings with FSB officers. He reports that the curriculum included political lectures with a heavy anti-Western bias, which led one of the students to suggest to his classmates that they 'unite and attack America' (Turovskiy, 2019: p. 184) and in 2017, the course organisers officially signed a contract for collaboration with the FSB Academy and the FSB administration in Moscow.

Various government agencies may also be using events such as online hackathons and large-scale conferences to identify cyber talent. An online contest called 'Digital Breakthrough', a product of Russia's 'Education' and 'Land of Opportunities' national initiatives, began in 2019 and included 40 regions and 66,000 participants (Zakharov, 2020). Both the FSB and GRU probably recruit from 'Positive Hack Days', which in 2014 hosted round-table discussions attended by FSB representatives on information security, the possibilities of network espionage and different countries' approaches to information security (Positive Hack Days, 2014). Dmitriy Badin, a GRU officer identified by the US and Germany for election-related hacking, very likely attended this event, probably at least in part to spot and recruit talent (RFE/RL, 2018).

Efforts to recruit capable computer science and IT specialists into Russia's military and security services probably offered lukewarm results and some evidence suggests direct outreach fails in certain cases. For example, insider accounts of the 'military science units' describe a lacklustre attempt at integrating technical talent into the ranks of Russia's military and accounts from 2015 from two science units describe inept leadership, ineffectual scientific work and frequent distractions that ranged from moving furniture to attending lectures on Stalin, which led some to conclude that the science units were largely a propaganda effort (Topwar.ru, 2015; Dobrynin, 2017). A separate account from 2017 claimed that most of the work performed by the Ministry of Emergency Services' science company was useless and its recruits even faced occasional physical hazing during their initial processing (Krasnaya Vesna, 2018). Additionally, the patriotic education that seemingly accompanies many efforts to directly recruit students into the military and security services probably dissuades a significant portion of potential recruits from joining. For example, a military veteran and former instructor for the KGB

in 2019 taught courses on 'psychotronic warfare' at one of Russia's largest technological universities that claimed social media 'was a weapon designed to destroy Russia' and the US High-Frequency Active Auroral Research Programme based in Alaska was a 'secret US mind-control project' (Yapporova, 2019). While the university's engineering and programming students largely bemoaned the mandatory courses, information security students praised their university's growing ties to the FSB and Federal Technical and Export Control Service, which offered internships and employment opportunities. Even beyond the propagandistic curricula, only 15 per cent of the 25,000 graduates of IT programmes in Russia are ready for immediate work, largely due to a shortage of professors with relevant skills, suggesting recruits to the military and security services probably require extensive training before they can contribute to operations or research (Izvestiya, 2019).

D. Bureaucratic Deconfliction

Inarguably, Moscow is incapable of controlling the wide range of exogenous factors that affect the health of its computing and IT industries, such as unanticipated phenomena like the coronavirus pandemic and fluctuations in oil prices, or the competitiveness of other states' hardware and software exports. The Russian government could, however, improve on many of the internal problems that affect the state's ability to optimise the resources and personnel at its disposal. Deconflicting missions between highly competitive Russian actors tasked with defending the country's networks and breaking into those of other states is an internal impediment to cyber operations that partly lies within Moscow's control. According to Kimberly Zenz, the Head of Threat Intelligence of the German Cyber Security Organisation (*Deutsche Cyber-Sicherheitsorganisation*), infighting among Russia's cyber actors has increased since 2014, resulting from factors that include geopolitical pressures, economic uncertainty, elite conflicts and shifting power from formal institutions (Zenz, 2019). In its most benign form, infighting results in duplicative and redundant efforts between actors and expending resources Moscow can ill-afford to waste. More significantly, infighting leads actors to leak information to undermine rival organisations, resulting in attribution or arrests. A leading theory behind the arrest by Russian authorities of the FSB's Centre for Information Security officers in late 2016 involves a plot by the centre's officers to undermine the GRU by leaking information about their 2016 operations to interfere in the US presidential election (Eckel, 2019).

Bureaucratic competition has long stifled Moscow's efforts to develop cyber capabilities. Even during the Soviet period, a zero-sum approach by state actors to fiscal and personnel resources ensured insurmountable bureaucratic hurdles for initiatives to enhance the nascent field of 'cybernetics' to further Moscow's goals related to defence and economic management (Peters, 2017). Within the modern FSB, at least occasional conflicts between the Centre for Information Security, a unit that conducts offensive operations, and the Communications Security Centre, largely responsible for ensuring cyber security, demonstrate the almost inevitable nature of bureaucratic friction even when official mandates and responsibilities avoid direct overlap (Rozh-

destvenskiy and Alekhina, 2017). The consistently independent operations by malware associated with Russia's military and intelligence services evidences a probable lack of collaboration. According to Check Point Research, a cyber security firm that investigated Russian state-sponsored malware in 2019, Russian state actors refrain from sharing their code with other actors and each maintained a team of malware developers working for years on 'parallel or similar' toolkits, that allowed researchers to 'spot redundancy in this parallel activity' (Cohen and Bassat, 2019). While compartmentalising these efforts may boost operational security, redundancy is something Moscow can ill afford considering how quantitatively outmatched Russian actors are by their rivals. By pooling resources between actors, or at least establishing rough divisions of labour, Moscow could improve offensive and defensive cyber operations.

To some extent, Russian officials have enacted means of reducing bureaucratic strife related to cyber capabilities. At a time when Moscow sought to rapidly build its cyber-capable cadres, the FSB and GRU overcame their deep-seated rivalry to secure an agreement in 2017 between the GRU's foremost cyber espionage unit, the 85th Main Special Service Centre (Unit 26165) and the FSB's prestigious cryptography academy, in which the latter would help train specialists for the former (RFE/RL, 2018). Often, firms contracted by state actors act as connective agents between various ministries and organisations, providing an at least unofficial and indirect path to cooperation between Russian actors.[10] Nevertheless, historical rivalries between the actors responsible for conducting cyber operations probably necessitate presidential mediation if Moscow hopes to foster lasting, collaborative relationships between them. Informal summits like the 2018 Siberian outing attended by FSB head Aleksandr Bortnikov, Minister of Defence Sergey Shoygu and President Putin offer a secure setting for such an inter-organisational parlay.

E. Espionage Targeting Other States' Cyber Capabilities

Of course, digital or traditional espionage offers a means of circumventing Russia's problems in developing its own capabilities by stealing the technology of other, more advanced states. Soviet intelligence has dedicated significant resources to science and technology espionage, such as the 'ente-erovtsy' (the phonetic pronunciation of the Russian acronym for science and technology intelligence, NTR) of the interwar period (Haslam, 2015). Probably no case serves as a better example of using espionage to gain offensive cyber capabilities than that of the Shadow Brokers, which reportedly involved probable Russian actors leveraging access to Kaspersky antivirus software and an NSA contractor's negligence to acquire malware that would eventually feed Russian and other state-backed offensive cyber operations (Harris, Lubold and Sonne, 2018). Although disconnected from state-sponsorship, the recent US Department of Justice (DOJ) indictment of a Russian

[10] Bloomberg's 2015 investigation into Kaspersky Labs provides a succinct, yet thorough snapshot of the interconnectedness of Russian state-backed cyber actors and the firms that support them (Matlack, Riley and Robertsom, 2015).

national who sought to extract sensitive information from a US company by using an inside agent to introduce malware into the company's network shows the continued vulnerability to espionage of the private sector which the West relies on to develop cyber capabilities (DOJ, 2020). Human-enabled cyber operations also lower the kind of offensive capabilities required to penetrate and exploit adversarial networks, either by providing sensitive details on cyber security infrastructure or by directly implanting malware into a targeted network. Herman Simm, a former Estonian intelligence officer who worked for Russia's Foreign Intelligence Service (SVR) until his arrest in 2008, provided Moscow with intimate details on NATO cyber security, leading the Alliance to conclude that Simm's leaks made NATO partners 'more vulnerable to cyber threats and attacks' (Schmid and Ulrich, 2010).

Nevertheless, there are obvious drawbacks in leaning too heavily on espionage to bolster Russia's lacklustre technological development. Even the best intelligence operations come to a usually abrupt end for various reasons, like an agent's reassignment, discovery by authorities or cessation in supporting their handlers, which limits intelligence services' insight into a particular field. The discovery of an agent network in a targeted country leads to diplomatic fallout, national embarrassment and typically strengthens counter-intelligence efforts among affected states and their allies. But the West has continuously shown its vulnerability to furtive computer espionage conducted remotely by China and Russia, a veritable backdoor into classified projects related to national security. The resemblance of Chinese fighter aircraft to US ones, for example, shows what prolonged access to these networks can yield for states engaging in cyber espionage (Daniels, 2017). Advanced Persistent Threats attributed by the cyber security community to Russian state actors have similarly gained access to sensitive information resting on NATO networks, such as APT28's longstanding targeting of US defence contractors (CISOMAG, 2020). The current environment in which Russian operators attempt to breach these networks, however, is somewhat different to many of these actors' past and largely undetected intrusions; an unprecedented level of international attention is now focused on malware attributed to Russia's military and intelligence services, which likely inhibits at least to some extent their ability to conduct cyber espionage. Underground or criminal malware, nonetheless, can provide original exploits disassociated with state-backed threat groups and intrusion sets. For example, malware widely attributed to a criminal group was possibly used in a campaign to illicitly acquire sensitive information on Ukrainian diplomacy and naval affairs shortly before the Kerch Strait incident in 2018, when Russian naval vessels apprehended and imprisoned Ukrainian mariners on the Black Sea (Tucker, 2018).

F. Concentrating on 'Information-Psychological' Effects

Russia is perhaps unique among contemporary cyber powers in its conceptualisation of the indivisibility of technical and psychological computer network operations, which range from offensive cyber operations on critical infrastructure to using false social media personas to disseminate messaging that supports Russian foreign policy or military objectives. As seamless as

this integration is among Russian security officials, operations like the use of Triton malware to shut down a Saudi energy facility in 2018 require far more technical development than the kind of digital psychological operations represented by, for instance, the GRU's limited use of Facebook in 2014 to sow social and political discontent in post-Maidan Ukraine. By concentrating on the latter, Russia's intelligence services and its military could employ more officers with less technical capabilities to conduct more less-technically intensive influence operations. One of Russia's longest-running influence campaigns on social media, dubbed by cyber security researchers 'Secondary Infektion', involves little more than registering single-use accounts on social media to amplify narratives published on alternative news websites and forums and posting simple forgeries of documents ostensibly written by Western or Ukrainian officials (Nimmo et al., 2020a). While concentrating on digital influence might come at the expense of developing emerging technologies needed for sophisticated offensive cyber operations, like those possibly needed in an unlikely wartime contingency with a conventional foe, Russian officials might be satisfied with an 'information-psychological' focus during a continued uneasy peace between Russia and the West. The riots in Novi Sanzhary, Ukraine, in early 2020 served as a stark example of the potential for Russian influence operations to inspire physical effects, however, few and circumstantially specific these cases may prove. The increasing social and political polarisation among states that Russian commonly targets with digital influence efforts might also reduce the need to illicitly procure sensitive documents, like those used by Russian actors to influence Western elections, as target audiences readily accept less credible forgeries that are easier to fabricate than obtaining actual sensational materials through cyber espionage.[11]

But evidence suggests that emerging technologies will affect digital influence operations as well, possibly blocking Russian techniques and capabilities that supported previous efforts. Despite, for example, the GRU's probable emphasis on using machine-translations to support digital psychological operations, the fact that linguistic mistakes have been frequently used to detect and identify their operations indicates technology has fallen short

[11] For instance, an early 2019 poll conducted by Gallup revealed that US President Donald Trump's job approval rating that year marked the most entrenched political polarisation within the US than previously recorded (Jones, 2019). At the same time, academic research has demonstrated a positive correlation between polarisation and receptivity to 'fake news', such as individuals' propensity to overrate the accuracy of news consistent with their political views (Sindermann, Cooper and Montag, 2020).

of ambition.[12] While Russian influence actors have recently demonstrated the ability to use 'deep fake' technology to create false social media profiles, such as the Internet Research Agency's (IRA) effort to support a covert website through a handful of inauthentic profiles (Macaulay, 2020), cyber security firms were able to quickly identify them. Indeed, emerging technologies thus far have probably benefitted NATO efforts to counter Russian digital influence operations than these technologies have forwarded Russian actors' ability to covertly conduct them. The Lithuanian website 'Demaskuok' (debunk), for instance, cooperated with Google in developing artificial intelligence capabilities to identify disinformation (President of the Republic of Lithuania, 2019). Given that both sides' implementation of emerging technologies to conduct and defend against digital influence campaigns is nascent, assessments about Russian capabilities allow for little more than low confidence estimations of their successful use. Nonetheless, Russia's fixation on conducting online influence operations, the proliferation of new and relevant technology, plus the apparent ability of other actors – particularly non-state ones – to use emerging technologies to influence audiences over the internet suggests Moscow is possibly better positioned to take advantage of these developments than those defending against its digital malign influence. As experts from the U.K.'s Conflict Studies Research Centre asserted:

> The introduction of machine learning and potentially artificial intelligence (AI), will vastly enhance capabilities for automating the reaching of mass audiences with tailored and plausible content. Consequently, they will render malicious actors even more powerful (Hartmann and Giles, 2020).

Just as human agents can advance cyber espionage and offensive cyber operations, they can help to overcome hurdles facing Russian digital influence campaigns such as a lack of cultural or linguistic expertise and the increasing ability of social media platforms to identify coordinated inauthentic behaviour. Both the GRU and SVR, for example, continue to solicit native authors to generate content on covertly run websites that aim to influence US audiences, including messaging about the upcoming presidential election, disinformation surrounding the coronavirus pandemic and exacerbating societal unrest (Barnes and Sanger, 2020). Similarly, Evgenniy Prigozhin's IRA as of September 2020 sought genuine American authors with partisan political viewpoints to write content for a website the IRA furtively managed,

[12] An official assigned to the GRU's main psychological warfare training programme at the Ministry of Defence's Military University (VUMO) sometime after the Georgian war claimed that his curriculum recently added classwork on 'machine-translations of literary texts into foreign languages' that would allow operators to quickly create 'high quality' translations of materials into foreign languages (Cheshuin, 2009). For examples of how linguistic mistakes have undermined GRU online influence operations, see the Atlantic Council's Digital Forensic Research Lab's report on 2016 operations, titled '#TrollTracker: Russia's Other Troll Team,' or Graphika's 2018 report on GRU use of blogs, including the 'non-native English' found in posts supporting the GRU's 'Inside Syria Media Centre' (Nimmo and Yap, 2018; Nimmo, Francois, Eib and Tamora, 2020b).

'peacedata.net'. The use of false social media accounts alerted Facebook and Twitter to the operation and eventually leading the social media platforms to disable the accounts and pages (BBC, 2020).

4. RECOMMENDATIONS AND CONCLUSION

The limitations affecting Moscow's drive to build a peer-worthy cyber force among its military and security services are unlikely to prevent them from continuing the cyber espionage, digital influence campaigns or even infrequent yet brazen attacks against critical infrastructure that have constituted their repertoire for at least the past two decades, though escalated amidst rising international tensions surrounding Russia's annexation of Crimea in 2014. Russian state actors behind these efforts will almost certainly find enough graduates of computer science and IT programmes to maintain current staffing and state actors will still be able to rely on support from independent IT and cyber security firms even as these sectors face growing challenges resulting from economic and demographic factors. In the highly unlikely event that Moscow faced imminent and overt conflict with NATO, these limitations would become more pronounced, as Russian services probably would be unable to match their adversary in terms of sustained and simultaneous offensive cyber operations, all while attempting to protect their own networks. Perhaps more importantly, Russia's cyber limitations will likely affect its ambitions to harness emerging technologies relevant to offensive and defensive capabilities.

In the meantime, Moscow will continue its cyber efforts in the face of quantitatively predominant adversaries, as one military author asserted, following renowned Russian military strategist Aleksandr Suvorov's axiom, 'not by number, but by skill' (Nesmeyanov, 2017). The countries targeted by Russian cyber operations at the same time can adopt measures to possibly exacerbate Russia's cyber limitations, such as depriving Russian actors of the skill prescribed by Suvorov. Most of Russia's young programmers, computer scientists and IT specialists hope to work abroad at least temporarily, primarily in the West. A 2018 poll by Gallup found that, among a record level of Russians hoping to emigrate, respondents named Germany and the US as their most-desired destinations (Moscow Times, 2019).[13] Indictments issued by the West against Russian state-backed hackers may do little to curb ongoing activity, but they probably dissuade at least some would-be military or intelligence officers from joining an agency that could permanently prevent their ability to travel to desirable countries. US Cyber Command's furtive messaging effort against Russian actors involved in digital influence operations, which revealed Cyber Command's awareness of Russian actors' personal information, presents a low-risk effort to exacerbate this issue. As much as Russian officials rely on the skill of their programmers, engineers

[13] A separate poll that year found that half of Russia's IT specialists wanted to emigrate, while Germany, the US and the U.K. were top choices for relocation (Strack et al., 2018).

and IT specialists to boost cyber capabilities,[14] they likely worry about their susceptibility to this kind of messaging. A long-serving Russian psychological operations officer warned as much in 2013, claiming that 'information-psychological' attacks on cyber operators constituted one of the three main types of cyber operations (Popov, 2013).

Sanctions offer an approach to limit Russian actors' ability to procure software and hardware, probably hindering state-backed efforts to conduct research related to emerging technologies, though possibly unnecessarily damaging private enterprise in Russia, including firms that are mostly unassociated with state programmes. Despite Moscow's intent to shift toward domestic software production, fuelled by sanctions levelled against Russia following its annexation of Crimea and by officials' fears that foreign software could benefit hostile cyber warfare aims, initiatives to spur domestic production quickly stalled, leading presidential spokesman Dmitriy Peskov to declare in 2016 that an effort to replace state agencies' use of Microsoft products was 'impossible for the time being, especially because local companies haven't yet developed worthy alternatives' (Popa, 2016). Around half of Russia's IT companies in 2017 felt that sanctions harmed their industry (Russoft, 2017b). While little evidence suggests that sanctions have an immediate effect on Russian state-sponsored cyber operations, with some experts claiming they actually spur more operations,[15] sanctions could provide a means of affecting Russian actors' long-term ability to adapt to an increasingly sophisticated operational environment. US sanctions, for instance, catalysed the downfall of a Russian tech company in 2018 that developed microprocessors as part of a state effort to reduce dependence on Western technology (Kolomychenko, 2018). Nevertheless, some experts state that sanctions imposed on Russia have benefitted its economy (Twigg, 2019), indicating that lasting sanctions could eventually spur enough domestic production to possibly support Moscow's cyber agenda. Moreover, the prolonged inability by Moscow to access needed foreign software and hardware could force Russian officials to overcome their entrenched suspicions of cooperating with Beijing on technological development, eventually forging a relationship that surpasses the existing programmes and bilateral initiatives. China and Russia this year took steps to reinforce their joint research on emerging technologies, such as a new research lab focused on artificial intelligence at the Moscow Institute of Physics and Technology sponsored by Huawei and mutual concerns—like antipathy toward the US—and benefits are likely to deepen technological ties between them (Bendett and Kania, 2020).

---

[14] As Dmitriy Mikhailov, the head of the Centre for Cybersecurity at the Russian National Research Nuclear University, explained in 2016, 'Russia has experienced some IT security problems, however our hackers are among the best in the world. In the case of cyber attacks, the most important thing is not related to material assets, but the skilful use [of] mathematical algorithms' (Gerden, 2016).

[15] According to Dmitri Alperovitch, the Chairman of the Silverado Policy Accelerator and former Chief Technology Officer of Crowdstrike, Russian state cyber actors as of 2015 used more brazen and frequent cyber espionage operations to compensate for Western sanctions levelled against Russia (Bennett, 2015).

Considering Russian actors' demonstrated ability to repurpose an adversary's malware to use in their own offensive operations, Western militaries and intelligence services should weigh the risks in using sophisticated malware in offensive operations. While Russian actors probably lack the personnel and resources needed to craft as many zero-day exploits as their rivals, they have consistently made use of malware purportedly developed by the US to conduct many of their operations, including the GRU's use of EternalBlue, attributed to the NSA, to carry out the NotPetya wiperware attack in 2017 (Hay Newman, 2018). Although US Cyber Command, for example, has shown a willingness to execute offensive operations as part of a new strategy to deter Russian offensive cyber operations, it could conceivably benefit Moscow by defending too far forward in cyberspace through the use of original malware that Russian actors can quickly reverse engineer and reuse. Similarly, Western militaries and intelligence services can help guard against Russia's ability to acquire proprietary exploits by enhancing operational security and access to relevant programmes, given Russian actors' consistent ability to take advantage of leaked or poorly secured offensive tools and malware developed by its rivals.

With the production of sophisticated tools available to NATO nations, member states need to ensure they incentivise reporting of vulnerabilities through, for example, bug bounty programmes across their industries. Such programmes, if properly compensated, could provide an alternative to selling such information underground. This can have a long-term crippling effect on illicit markets for vulnerabilities and restrict the ability of Russia state-supported cyber threats to access and exploit them (Supreme Headquarters Allied Power Europe (SHAPE) representative 2018, pers. comm., 12 August).

There is little reason to doubt Russian actors' capability to continue offensive cyber operations, digital influence operations and cyber espionage operations in the near-term future. There is sufficient evidence, however, to doubt Moscow's ability to adapt to emerging technologies that require intensive research and investment that exceed the state's capacity. Although Moscow could overcome some of the challenges affecting cyber development such as bureaucratic competition, reducing corruption or alleviating the culture shock that programmers and IT specialists face when entering the military or security services, Russian officials can do little to influence the exogenous factors likely to affect the health of Russia's IT and computing industries on which the state relies to advance its capabilities. These limitations provide only narrow openings for countries affected by Russian cyber activity to affect Russia's future capabilities, like dissuading potential recruits from joining Russia's military or security services by barring them from the countries in which many Russian IT and computer science specialists hope to work or travel. Efforts such as this will almost certainly fail to prevent the next NotPetya attack, a type of behaviour that can only be resolved through deterrence, diplomacy or a drastic change in tensions between the West and Mos-

cow. But indictments and sanctions could to some degree inhibit Moscow's ability to use emerging technologies like quantum computing and artificial intelligence for future offensive operations. At the same time, Western cyber planners should pay more attention to economic and demographic factors, such as the outflow of technological talent from Russia, which will shape how Moscow approaches cyber competition with its perceived adversaries throughout the next decade.

5. REFERENCES

Ali, R. (2017) NATOs Little Noticed but Important New Aggressive Stance on Cyber Weapons. *Foreign Policy*. 7 December. Available from: https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/ [Accessed 21st October 2020].

Appell, J. (2015) The Short Life and Speedy Death of Russia's Silicon Valley. *Foreign Policy*. 6 May. Available from: https://foreignpolicy.com/2015/05/06/the-short-life-and-speedy-death-of-russias-silicon-valley-medvedev-go-russia-skolkovo/ [Accessed 21st October 2020].

Barnes, J. E. & Sanger, D. E. (2020) Russian Intelligence Agencies Push Disinformation on Pandemic. *The New York Times*. 28 July. Available from: https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html [Accessed 21st October 2020].

BBC News. (2020) Facebook and Twitter 'dismantle Russian network'. 2 September. Available from: https://www.bbc.com/news/world-us-canada-53980979 [Accessed 21st October 2020].

Bennett, C. (2015) Russia's cyberattacks grow more brazen. *The Hill*. 12 April. Available from: https://thehill.com/policy/cybersecurity/238518-russias-cyberattacks-grow-more-brazen [Accessed 21st October 2020].

Bendett, S. & Kania, E. (2020) The Resilience of Sino-Russian High-Tech Cooperation. *War on the Rocks*. 12 August. Available from: https://warontherocks.com/2020/08/the-resilience-of-sino-russian-high-tech-cooperation/ [Accessed 21st October 2020].

Beshaj, L & Hall, A.O. (2020), Recent developments in cryptography. In Jančárková, T., Lindström, L., Signoretti, M., Tolga, I., & Visky, G. (eds.), *12th International conference on cyber conflict, 20/20 vision: The next decade*. NATO CCDCOE Publications, Tallinn, pp. 351-368.

Bodner, M. (2015) Russian Military Launches Cybertraining Programme for Youth. *The Moscow Times*. 1 September. Available from: https://www.themoscowtimes.com/2015/09/01/russian-military-launches-cybertraining-program-for-youth-a49276 [Accessed 21st October 2020].

Cheshuin, S. A. (2009) *Osobennosti sovremennovo informatsionnovo protivoborstva i ikh uchod pri podgotovke spetsialistov zarubezhnoy voennoy informatsii v voennom universitete* [The Features of Modern Information Confrontation During the Training of Specialists of foreign Military Information at the Military University]. Available from: http://www.milpol.ru/sgs/sgs.html [Accessed 21st October 2020].

Cimpanu, C. (2019) The world's most famous and dangerous APT (state-developed) malware. *ZDNet*, 8 July. Available from: https://www.zdnet.com/pictures/the-worlds-most-famous-and-dangerous-apt-state-developed-malware/ [Accessed 21st October 2020].

CISOMAG. (2020) Russian Hackers Attempting Cyber Espionage Against Middle East Defence Firms. 24 March. Available from: https://cisomag.eccouncil.org/russian-hackers-attempting-cyber-espionage-against-middle-east-defense-firms/ [Accessed 21st October 2020].

Cohen, I. & Bassat, O. B. (2019) Mapping the connections inside Russia's APT Ecosystem. *Check Point Research*. 24 September. Available from: https://research.checkpoint.com/2019/russianaptecosystem/ [Accessed 21st October 2020].

Council on Foreign Relations. Turla. Available from: https://www.cfr.org/cyber-operations/turla [Accessed 21st October 2020].

Daniels, J. (2017) Chinese theft of sensitive US military technology is still a huge problem, says defence analyst. *CNBC*. 8 November. Available from: https://www.cnbc.com/2017/11/08/chinese-theft-of-sensitive-us-military-technology-still-huge-problem.html [Accessed 21st October 2020].

Dobrynin, S. (2017) Rosgiki dlya Rosgvardiya [Rosgiki for the Russian National Guard]. *Radio Svoboda/Radio Liberty*, 27 July 27. Available from: https://www.svoboda.org/a/28643436.html [Accessed 21st October 2020].

Dylevskiy, I. N., Komov, S. A., & Petrunin, A.N. (2013) Ob Informatsionnykh Aspektakh Mezhdunarodno-Pravovo Ponyatiya Agressiya [On the Informational Aspect of the International-Legal Understanding of Aggression]. *Voennaya Mysl*. 10, 3-12.

Eckel, M. (2019) In Moscow Treason Trial, A Major Scandal for Russian Security Agency. *RFE/RL*. 27 February. Available from: https://www.rferl.org/a/russia-hacker-mikhailov-stoyanov-fsb-scandal-for-russian-security-agency/29794092.html [Accessed 21st October 2020].

FireEye, Inc. (2014) APT28: A Window into Russia's Cyber Espionage Operations? Available from: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf [Accessed 21st October 2020].

Fond Perspektivykh Issledovaniy. (2019a) *Konkursy [Contests]*. Available from: https://fpi.gov.ru/tenders/184/ [Accessed 21st October 2020].

Fond Perspektivykh Issledovaniy. (2019b) *Protokol No. 2 zasedaniya konkursnoy komissii [Protocol No. 2 of the Contest Commission Session]*. 31 May. Available from: https://fpi.gov.ru/upload/iblock/de3/de33a1a0b32c2b2abbe2c9013eb853a3.pdf [Accessed 21st October 2020].

Gerden, E. (2016) Russia to spend $250m strengthening cyber-offensive capabilities. *SC Media*. February 4. Available from: https://www.scmagazineuk.com/russia-spend-250m-strengthening-cyber-offensive-capabilities/article/1477698 [Accessed 21st October 2020].

Greenberg A. (2019) *Sandworm*. New York: Doubleday.

Hay Newman, L. (2018) The Leaked NSA Spy Tool That Hacked the World. *WIRED*. 7 March. Available from: https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/ [Accessed 21st October 2020].

Harris, S., Lubold, G. & Sonne, P. (2018) How Kasperskys Software Fell Under Suspicion of Spying on America. *The Wall Street Journal*. January 5. Available from: https://www.wsj.com/articles/how-kasperskys-software-fell-under-suspicion-of-spying-on-america-1515168888 [Accessed 21st October 2020].

Harris, S. & Barrett, D. (2019) Justice Department investigates Sci-Hub founder on suspicion of working for Russian intelligence. *The Washington Post*. 19 December. Available from: https://www.washingtonpost.com/

national-security/justice-department-investigates-sci-hub-founder-on-suspicion-of-working-for-russian-intelligence/2019/12/19/9dbc-b6e6-2277-11ea-a153-dce4b94e4249_story.html [Accessed 21st October 2020].

Hartmann, K. & Giles, K. (2020) The Next Generation of Cyber-Enabled Information Warfare. In Jančárková, T., Lindström, L., Signoretti, M., Tolga, I., & Visky, G. (eds.), *12th International conference on cyber conflict, 20/20 vision: The next decade*. NATO CCDCOE Publications, Tallinn, pp. 233-249.

Haslam, J. (2015) *Near and Distant Neighbours: A New History of Soviet* Intelli*gence*. New York: Farrar Strauss and Giroux.

Heller, M. (2018) Durov refuses to hand over Telegram encryption keys to FSB. *TechTarget*. 21 March. Available from: https://searchsecurity.techtarget.com/news/252437323/Dorov-refuses-to-hand-over-Telegram-encryption-keys-to-FSB [Accessed 21st October 2020].

Herbst, J. & Erofeev, S. (2019) *The Putin Exodus: The New Russian Brain Drain*. The Atlantic Council, Eurasia Center. Available from: https://publications.atlanticcouncil.org/putin-exodus/The-Putin-Exodus.pdf [Accessed 21st October 2020].

Howells, L. & Kalfoglou, Y. (2020) Security Think Tank: AI cyber attacks will be a step-change for criminals. *Computer Weekly*. 2 July. Available from: https://www.computerweekly.com/opinion/Security-Think-Tank-AI-cyber-attacks-will-be-a-step-change-for-criminals [Accessed 21st October 2020].

International Military-Technical Forum 'Army-2018'. (2018) A Strategy for the Development of Technologies in the Sphere of Artificial Intelligence for the National Security of the Russian Federation. 24 August 2018. Moscow region. Russia (held at the Patriot Expo).

Izvestiya. (2019) Nazvany zarplaty IT-spetsialistov v Rossii [The salaries of IT-specialists in Russia have been announced]. *Izvestiya*. 13 September. Available from: https://iz.ru/920869/2019-09-13/nazvany-zarplaty-it-spetcialistov-v-rossii [Accessed 21st October 2020].

Jones, J. M. (2019) Trump Job Approval Sets New Record for Polarisation. *Gallup*. 16 January. Available from: https://news.gallup.com/poll/245996/trump-job-approval-sets-new-record-polarisation.aspx [Accessed 21st October 2020].

Katwala, A. (2018) Why Chinas perfectly placed to be quantum computing's superpower. *WIRED*. 14 November. Available from: https://www.wired.co.uk/article/quantum-computing-china-us [Accessed 21st October 2020].

Khodarenok, M. & Zatari A. (2017) Kibervoyna: chem opasny lyudi s noutbukami [Cyberwarfare: why people with notebooks are dangerous]. *Gazeta.ru*. 27 August. Available from: https://www.gazeta.ru/army/2017/08/26/10859996.shtml [Accessed 21st October 2020].

Kolomychenko, M. (2017) U kiberbezopasnosti menyaetsya curator [Cybersecurity is changing its director]. *Kommersant*. 13 January. Available from: https://www.kommersant.ru/doc/3189312 [Accessed 21st October 2020].

Kolomychenko, M. (2018) Exclusive: Russian high tech project flounders after US sanctions. *Reuters*. 17 October. Available from: https://www.reuters.com/article/us-russia-usa-sanctions-technology-exclu/exclusive-russian-high-tech-project-flounders-after-u-s-sanctions-idUSKCN1MR1LF [Accessed 21st October 2020].

Korotaev, V. (2017) V internet vveli kibervoyska [A cyberforce was introduced to the internet]. *Kommersant*, 10 January. Available from: https://www.kommersant.ru/doc/3187320 [Accessed 12th November 2020].

Kottasova, I. (2017) Why Russia's cyber defences are so weak. *CNN*. 15 May. Available from: https://money.cnn.com/2017/05/15/technology/russia-vulnerable-cyberattack/index.html [Accessed 21st October 2020].

Kozlov, V. (2020) Russian Tech Industry Faces Coronavirus Brain Drain. *The Moscow Times*. 17 June. Available from: https://www.themoscowtimes.com/2020/06/17/russian-tech-industry-faces-coronavirus-brain-drain-a70607 [Accessed 21st October 2020].

Kramer, A. E. (2016) How Russia Recruited Elite Hackers for Its Cyberwar. *New York Times*. 29 December. Available from: https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html [Accessed 21st October 2020].

Kramer A. E. (2017) Hacker Is a Villain to Russia and the United States, for Different Reasons. *New York Times*. 16 March. Available from: https://www.nytimes.com/2017/03/16/world/europe/russian-hacker-fsb-agent-dmitry-dokuchaev.html [Accessed 21st October 2020].

Krasnaya Vesna. (2018) Bolshaya chast raboty nauchnykh rot ukhodit v stol [The majority of science companies work is useless]. *Krasnaya Vesna.* 24 February. Available from: https://rossaprimavera.ru/news/6cccb188 [Accessed 21st October 2020].

Kremlin.ru. (2006) Poslanie Federalnomu Sobraniyu Rossiyskoy Federatsii [Address to the Federal Assembly of the Russian Federation]. 10 May. Available from: http://kremlin.ru/events/president/transcripts/23577 [Accessed 21st October 2020].

Lata, V. F., Annenkov, V.A. & Moiseev, V.F. (2019) *Informatsionnoe Protivoborstvo: Sistema Terminov i Opredelenniy* [Information Confrontation: A System of Terms and Definitions]. *Vestnik Akademii Voennykh Nauk.* 2 (67), 128-38.

Lenta.ru. (2017) Byvshiy sotrudnik voennovo NII osuzhden za khishchenie radiodetaley na 40 millionov [A former worker of a military research institute was sentenced for stealing radio equipment worth 40 million]. *Lenta*. 31 January. Available from: https://lenta.ru/news/2017/01/31/radiodetali/ [Accessed 21st October 2020].

Levin, I. I. (2004). *Metody I programmno-apparatnye sredstva parallelnykh strukturno-protsedurnykh vychislenniy* [Methods and software and hardware for parallel structural-procedural computations]. Doctor of Technical Science Dissertation. Taganrog State Radio-Technical University.

Lysenko, V. & Brooks, C. (2018) Russian information troops, disinformation and democracy. *First Monday*. 23 (5). Available from: https://firstmonday.org/article/view/8176/7201 [Accessed 12th November 2020].

Macaulay, T. (2020) Russia's most notorious troll farm reportedly used deepfakes to push a fake news outlet on Facebook. *The Next Web*. 2 September. Available from: https://thenextweb.com/neural/2020/09/02/russias-most-notorious-troll-farm-reportedly-used-deepfakes-to-push-a-fake-news-outlet-on-facebook/ [Accessed 21st October 2020].

Markotkin, N. & Chernenko, E. (2020) *Developing Artificial Intelligence in Russia: Objectives and Reality*. Carnegie Moscow Center. 5 August. Available from: https://carnegie.ru/commentary/82422 [Accessed 16th November 2020].

Marks, J. (2020) The Cybersecurity, 202: Chinese hackers could work for the gov-

ernment – or themselves. *The Washington Post*. 22 July. Available from: https://www.washingtonpost.com/politics/2020/07/22/cybersecurity-202-chinese-hackers-could-work-government-or-themselves/ [Accessed 21st October 2020].

Matlack, C., Riley, M. & Robertson, J. (2015) The Company Securing Your Internet Has Close Ties to Russian Spies. *Bloomberg*. 19th March. Available from: https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies [Accessed 21st October 2020].

Maurer, T. (2018) Why the Russian Government Turns a Blind Eye to Cybercriminals. *Slate*. 2 February. Available from: https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html [Accessed 21st October 2020].

Maurer, T & Hinck, G. (2018) Russia's Cyber Strategy. *ISPI Online*. 21 December. Available from: https://www.ispionline.it/it/pubblicazione/russias-cyber-strategy-21835 [Accessed 21st October 2020].

Melkozerova, V. & Parafeniuk, O. (2020) How coronavirus disinformation caused chaos in a small Ukrainian town. *NBC News*. 3 March. Available from: https://www.nbcnews.com/news/world/how-coronavirus-disinformation-caused-chaos-small-ukrainian-town-n1146936 [Accessed 21st October 2020].

Miller, C. (2020) A Small Town Was Torn Apart by Coronavirus Rumors. *Buzzfeed News*. 9 March. Available from: https://www.buzzfeednews.com/article/christopherm51/coronavirus-riots-social-media-ukraine [Accessed 21st October 2020].

Modestov, S. (1997). *SShA gotovy k informatsionnoy voyne s Rossiey* [The US is ready for an information war with Russia]. *Nezavisimoe Voennoe Obozrenie*. 52 (25), pp. 15-23.

The Moscow Times. (2015) Russia's DARPA Working on Underwater Battlebots to Protect Coastline. *The Moscow Times*. 8 July. Available from: https://www.themoscowtimes.com/2015/07/08/russias-darpa-working-on-underwater-battlebots-to-protect-coastline-a48005 [Accessed 21st October 2020].

The Moscow Times. (2019) Record Number of Russians Want to Emigrate – Gallup. *The Moscow Times*. 4 April. Available from: https://www.themoscowtimes.com/2019/04/04/record-number-of-russians-want-to-emigrate-gallup-a65092 [Accessed 21st October 2020].

Nakashima, E. & Warrick, J. (2012) Stuxnet was work of US and Israeli experts, officials say. *The Washington Post*. 2 June. Available from: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html [Accessed 21st October 2020].

National Association for International Information Security (NAIIS). (2020) *Management of the Association*. Available from: http://namib.online/en/president-of-naiis/ [Accessed 21st October 2020].

National Security Agency (NSA) & The Federal Bureau of Investigation (FBI). (2020) NSA and FBI Expose Russian Previously Undisclosed Malware "Drovorub" in Cybersecurity Advisory. *Press Room*. 13 August. Available from: https://www.nsa.gov/news-features/press-room/Article/2311407/nsa-and-fbi-expose-russian-previously-undisclosed-malware-drovorub-in-cybersecu/ [Accessed 16 November 2020].

Nesmeyanov, V. (2017) *Eta tikhaya, smertelnaya voyna* [This quiet, deadly war]. *Flag Rodiny*. 17 (27273), p. 7.

Nimmo, B. & Yap, N. (2018) #TrollTracker: Russia's Other Troll Team. *Digital Forensic Research Lab*. 2 August. Available from: https://medium.com/dfrlab/trolltracker-russias-other-troll-team-4efd2f73f9b5 [Accessed 21st October 2020].

Nimmo, B., Francois, C., Eib, S. & Tamora, L. (2020a). *From Russia With Blogs*. Graphika. Available from: https://public-assets.graphika.com/reports/graphika_report_from_russia_with_blogs.pdf [Accessed 21st October 2020].

Nimmo, B., Francois, C., Eib, S. & Tamora, L. (2020b) *Secondary Infektion*. Graphika. Available from: https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf [Accessed 21st October 2020].

Office of the Director of National Intelligence (ODNI). (2020) *The U.S. Intelligence Community Budget*. Available from: https://icontherecord.tumblr.com/ic-budget [Accessed 16 November 2020].

Peters, B. (2017) *How Not to Network a Nation: The Uneasy History of the Soviet Internet.* MIT Press: London.

Peterson, D. J. (2005). *Russia and the Information Revolution*. Santa Monica: RAND Corporation. Available from: https://www.rand.org/pubs/monographs/MG422.html [Accessed 21st October 2020].

Pomerleau, M. (2018) Here are the cyber staffing issues facing the Defence Department. *Fifth Domain*. August 3. Available from: https://www.fifthdomain.com/dod/cybercom/2018/08/03/can-cyber-command-overcome-its-staffing-shortage/ [Accessed 21st October 2020].

Popa, B. (2016) Russian President Spokesman Says It's Impossible to Give Up on Foreign Software. *Software Russia*. 4 November. Available from: http://www.software-russia.com/in_focus/media/russian-president-spokesman-says-it-is-impossible-to-give-up-on-foreign-software [Accessed 21st October 2020].

Popov, I. M. (2013) Vzglyad na deystviya v kiberprostranstve pod voennym uglom zreniya [A military perspective on actions in cyberspace]. *Nezavisimoe Voennoe Obozrenie*. 13 December. Available from: https://nvo.ng.ru/concepts/2013-12-13/1_war.html [Accessed 21st October 2020].

Positive Hack Days (Phd). (2014) *Best of PHDays*, 2014. Available from: http://2014.phdays.ru/ [Accessed 21st October 2020].

Press Office of the President of the Republic of Lithuania. (2019) *Fight against disinformation is EU priority*. Available from: https://www.lrp.lt/en/media-center/news/fight-against-disinformation-is-eu-priority/32098 [Accessed 21st October 2020].

Radio Free Europe/Radio Liberty. (2017) Putin Compares Hackers to Artists, Says They Could Target Russia's Critics For Patriotic Reasons. *RFE/RL*. 1 June. Available from: https://www.rferl.org/a/russia-putin-patriotic-hackers-target-critics-not-state/28522639.html [Accessed 21st October 2020].

Radio Free Europe/Radio Liberty. (2018) Investigative Report: On the Trail of the 12 Indicted Russian Intelligence Officers. *RFE/RL*. 19 July. Available from: https://www.rferl.org/a/investigative-report-on-the-trail-of-the-12-indicted-russian-intelligence-officers/29376821.html [Accessed 21st October 2020].

RBC.ru. (2017) Medvedev nazval nedopustimym eksport intellekta iz Rossii [Med-

vedev called the export of intellect from Russia unacceptable]. *RBC.ru*. 27 February. Available from: https://www.rbc.ru/rbcfreenews/58b41aec9a7947ea101ed916 [Accessed 21st October 2020].

RBC.ru. (2018) Rogozin prisval ostanovit vymyvanie mozgov za rubezh [Rogozin urged a stop to brain drain abroad]. *RBC.ru.* 27 February. Available from: https://www.rbc.ru/rbcfreenews/5a9524119a794717e2d20506 [Accessed 21st October 2020].

Reuters. (2017) WannaCry Ransomware Hit Some Russian Banks. *Fortune*. 19 May. Available from: https://fortune.com/2017/05/19/wannacry-ransomware-russia/ [Accessed 21st October 2020].

Romanova, S. (2018) Rekrutery vyyasnili prichiny otezda rossiyskikh IT-spetsialistov za rubezh [Recruiters revealed the reasons for the departure of Russian IT specialists abroad]. *RBC.ru.* 5 June. Available from: https://www.rbc.ru/rbcfreenews/5b168d0e9a7947958ec9dcf3 [Accessed 21st October 2020].

Rozhdestvenskiy, I. & Alekhina, M. (2017) Predatelstvo v FSB: shto izvestno ob arestakh v spetsluzhbe i u Kasperskovo [Betrayal in the FSB: What is known about the arrests in the special service and Kaspersky]. *RBC.ru.* 25 January. Available from: https://www.rbc.ru/society/25/01/2017/58887a2b9a794770370e0d9a [Accessed 21st October 2020].

Russoft. (2017a) Russoft: programmisty nedovolny urovnem svoevo dokhoda [Russoft: programmers are unhappy with their income]. *Russoft*. 13 December. Available from: http://old.russoft.ru/smi/4331 [Accessed 21st October 2020].

Russoft. (2017b) Issledovanie: Okolo 50% Rossiyskikh IT-kompaniy negativno otsenivayut vliyanie sanktsiy na industriyu [Research: About 50% of Russian IT-companies assess sanctions had a negative impact on the industry]. *Russoft*. 7 May. Available from: http://old.russoft.ru/smi/3955 [Accessed 21st October 2020].

Russoft. (2019) *16th Annual Survey: 2019 Russian Software Industry*. Available from: https://russoft.org/wp-content/uploads/2019/12/RUSSOFR-Survey-ENG-2019.pdf [Accessed 21st October 2020].

Sayfetdinov, K. I. (2014) Informatsionnoe Protivoborstvo v Voennoy Sfere [Information Confrontation in the Military Sphere]. *Voennaya Mysl*. 7, 38-41.

Satter, R. & Bodner, M. (2018) Leaked chats show alleged Russian spy seeking hacking tools. *Associated Press*, 1 August. Available from: https://apnews.com/aa719ede3637469a91da829c551fe81b/Leaked-chats-show-alleged-Russian-spy-seeking-hacking-tools [Accessed 21st October 2020].

Schmid, F. & Ulrich, A. (2010) New Documents Reveal Truth on NATOs Most Damaging Spy. *Spiegel International*. 30 April. Available from: https://www.spiegel.de/international/europe/betrayer-and-betrayed-new-documents-reveal-truth-on-nato-s-most-damaging-spy-a-691817.html [Accessed 21st October 2020].

Shurygin, D. (2018) Putin vysoko otsenil tekhnopolis ERA v Anape [Putin highly valued the ERA technopolis in Anapa]. *TV Zvezda.* 22 November. Available from: https://tvzvezda.ru/news/opk/content/201811221606-8wkd.htm [Accessed 21st October 2020].

Sindermann, C., Cooper, A. & Montag, C. (2020) A short review on susceptibility to falling for fake political views. *Current Opinion in Psychology*. 36, 44-8.

Skobelev, Vladislav. (2020) Kasperskaya predupredila Mishustina ob emigratsii IT-spetsialistov za rubezh (Kasperskaya warned Mishustin about the

emigration of IT specialists abroad) *RBC.ru*. 3 June. Available from: https://www.rbc.ru/technology_and_media/03/06/2020/5ed665499a7947fd676d0462 [Accessed 21st October 2020].

Smith-Goodson, P. (2019) Quantum USA Vs. Quantum China: The World's Most Important Technology Race. *Forbes*. 10 October. Available from: https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/#d91d24072de9 [Accessed 21st October 2020].

Strack, R., Kovacs-Ondrejkovic, O, Antebi, P., Schudey, A., Ignatova, M., & Oblov, A. (2018) *Russia Faces a Talent Conundrum*. Boston Consulting Group. Available from: https://www.bcg.com/publications/2018/russia-faces-talent-conundrum-global-talent [Accessed 21st October 2020].

Stubbs, J. (2017) NotPetya hackers likely behind BadRabbit attack: researchers. *Reuters*. 26 October. Available from: https://www.reuters.com/article/us-cyber-attack-russia/notpetya-hackers-likely-behind-badrabbit-attack-researchers-idUSKBN1CV1TI [Accessed 21st October 2020].

TASS. (2020) Innovation center Skolkovo is not Silicon Valley's counterpart – directors board chair. *TASS*. 2 June. Available from: https://tass.com/science/1163251 [Accessed 21st October 2020].

TASS. (2020) Not Chasing IBM and Google: Russian scientists work on independent quantum computer. *TASS*. 22 January. Available from: https://tass.com/science/1111769 [Accessed 21st October 2020].

Topwar.ru. (2015) Pro sluzhbu v nauchnoy rote [About service in a science company]. *Topwar*. 26 December. Available from: https://topwar.ru/88239-pro-sluzhbu-v-nauchnoy-rote.html [Accessed 21st October 2020].

Troianovski, A. & Nakashima, E. (2018) How Russia's military intelligence agency became the covert muscle in Putin's duels with the West. *Washington Post*. 28 December. Available from: https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html [Accessed 21st October 2020].

Tucker, P. (2018) Russia Launched Cyber Attacks Against Ukraine Before Ship Seizures, Firm Says. *Defence One*. 7 December. Available from: https://www.defenseone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153375/ [Accessed 21st October 2020].

Turovskiy, D. (2019) *Vtorzhenie: Kratkaya istoriya Russkikh khakerov (Invasion: A short history of Russian hackers)* Moscow, Inviduum.

Turovsky, D. (2018) It's our time to serve the Motherland: How Russia's war in Georgia sparked Moscow's modern-day recruitment of criminal hackers. *Meduza*. 7 August. Available from: https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland [Accessed 21st October 2020].

Twigg, J. (2019) Russia is Winning the Sanctions Game. *The National Interest.* 14 March. Available from: https://nationalinterest.org/blog/skeptics/russia-winning-sanctions-game-47517 [Accessed 21st October 2020].

Uppal, R. (2019) Russia's Advanced Research Foundation Aims Breakthrough High-Risk Research and Development Like US DARPA. *International Defence, Security & Technology.* February 2. Available from: https://webcache.googleusercontent.com/search?q=cache:Qh3ahoZLDJIJ:Available from: https://idstch.com/industry/russia-s-advanced-research-foundation-advancing-as-an-answer-to-us-darpa/+&cd=1&hl=en&ct=clnk&gl=us [Accessed

21st October 2020].

US Department of Justice. (2020) Russian National Indicted for Conspiracy to Introduce Malware into a Computer Network. *Office of Public Affairs*. 4 September. Available from: https://www.justice.gov/opa/pr/russian-national-indicted-conspiracy-introduce-malware-computer-network [Accessed 21st October 2020].

US Department of the Treasury. (2019) Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware. *Press Releases*. 5 December. Available from: https://home.treasury.gov/news/press-releases/sm845 [Accessed 21st October 2020].

US Government Publishing Office. (2014) Hearing on National Defense Authorization Act for Fiscal Year 2015 And Oversight of Previously Authorized Programs before the Committee on Armed Services. *House of Representatives, One Hundred Thirteenth Congress, Second Session.* Available from: https://www.govinfo.gov/content/pkg/CHRG-113hhrg87867/html/CHRG-113hhrg87867.htm [Accessed 16 November 2020].

Vyalykh, S. A. (1999) *Povyshenie effektivnosi zashchity avtomatizirovannykh sistem operativnovo upravleniya ot vredonosnykh programmnykh vozdeystviy* [Raising the effectiveness of automated operational control system defence from the impact of malicious software]. Candidate of Technical Sciences Dissertation. 5th Central Scientific Research Test Institute.

Vesti.ru. (2019) Putin posetil ekspozitsiyu tekhnopolisa Era na forume Armiya, 2019 [Putin visited an exhibition of Era technopolis at the Army, 2019 forum]. *Vesti.ru.* 27 June. Available from: https://www.vesti.ru/article/1321178 [Accessed 21st October 2020].

Villalon, A. (2016) The Russian ICC (V): FSB. *Security at Work*. 20 December. Available from: https://www.securityartwork.es/2016/12/20/the-russian-icc-v-fsb/ [Accessed 21st October 2020].

Wezeman, S. T. (2020) Russia's military spending: Frequently asked questions. Available from: https://www.sipri.org/commentary/topical-backgrounder/2020/russias-military-spending-frequently-asked-questions [Accessed 21st October 2020].

Yapporova, L. (2019) Conspiracy U: A former KGB instructor is winning over students with pseudoscience lectures and FSB internships. *Meduza*. 27 December. Available from: https://meduza.io/en/feature/2019/12/27/conspiracy-u [Accessed 21st October 2020].

Zakharov, R. (2020) V Rossii startoval perviy onlain-khakaton konkursa tsifrovoy proryv [The first online hackathon contest digital breakthrough was started in Russia]. *Zvezda*. 5 June. Available from: https://public.tvzvezda.ru/news/t/2020651844-5qDBr.html [Accessed 21st October 2020].

Zenz, K. (2019) Infighting Among Russian Security Services in the Cyber Sphere [Powerpoint Presentation]. *Black Hat USA*. August. Available at: Available from: https://i.blackhat.com/USA-19/Thursday/us-19-Zenz-Infighting-Among-Russian-Security-Services-in-the-Cyber-Sphere.pdf [Accessed 21st October 2020].

Zetter, K. (2014) *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.

Cyberspace Escalation: Ladders or Lattices?

Martin C. Libicki
Maryellen and Richard L. Keyser Distinguished Visiting Professor
Center for Cyber Security Studies
United States Naval Academy

Olesya Tkacheva
Assistant Professor
Department of International Affairs
Vesalius College and Free University of Brussels (VUB)

Abstract: In any domain, deliberate escalation or de-escalation is an important tool in the management of crisis and conflict. Adroit use of such a tool to communicate intention and resolve presumes that all sides share an understanding that a move from one condition to another is or is not escalatory or de-escalatory. We argue that in cyberspace the distinction between the escalatory and de-escalatory use of cyber capabilities is less straightforward. It is more appropriate to conceptualise escalation as evolving like a lattice, allowing horizontal spill over to other domains as well as vertical movement that corresponds to greater intensity of conflict. We offer conceptual scenarios to illustrate this point and discuss the implications for NATO's doctrine for joint cyber operations and risk management.

Keywords: *NATO, cyber escalation, offensive cyber, cyber warfare*

1. Cyberspace Escalation: Ladders or Lattices?

In any domain, deliberate escalation or de-escalation is an important tool in the management of crisis and conflict. Adroit use of such a tool to communicate intention and resolve presumes that all sides share an understanding that a move from one condition to another is escalatory or de-escalatory. We contend, however, that cyberspace operations may challenge such understanding, looking like escalation in some respects but like the status quo or de-escalation in others. Such ambiguity should be appreciated by organisations such as NATO. Since the declaration of cyberspace as

a military domain at its 2016 Warsaw Summit, NATO has upgraded its capabilities and updated its institutional and legal frameworks to operate in cyberspace as effectively as in other domains. This has entailed, among other measures, establishing a Cyberspace Operations Centre (CyOC) and integrating Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) into NATO operations. These allow the Allies to voluntarily contribute cyber capabilities to NATO missions to achieve desired effects while retaining command and control over them. Although NATO does not have its own offensive cyber capabilities, the growing importance of cyber operations for NATO's effective collective defence and deterrence requires a thorough understanding of how deploying cyber capabilities may affect conflict dynamics. It remains to be seen whether this will be perceived by conflicting parties as escalatory or de-escalatory.

The need to assess the implications of cyber for conflict dynamics is stated clearly in the *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations*. This requires the consideration of interdependencies between cyber and other operational domains when evaluating the intended and unintended consequences of using cyber capabilities and also emphasizes the importance of risk management (NATO, 2020: p. 25). The doctrine, however, is devoid of any guidance on how to handle escalation in cyberspace. As noted in 2017 by Jamie Shea, the Deputy Assistant General for Emerging Threats:

> Whereas we have a good idea of how to deter a nuclear or conventional attack, to deal with crises in the traditional domains, to employ arms control or confidence-building arrangements, we still do not have a good idea of how to deter or respond to major cyber attacks (Shea, 2017: p. 27).

This chapter illustrates why risk management in cyberspace could be more complicated than in other domains due to an inherited ambiguity about the escalatory or de-escalatory effects of cyber operations. We offer hypothetical scenarios to illustrate this point and then a model of escalation in cyberspace. Whereas previous studies have conceptualised escalation as changes in conflict intensity illustrated by the metaphor of an escalation 'ladder', our model characterises cyber escalation as a lattice. We show that escalation management strategies that assume escalation to be a ladder rather than a lattice may not work as expected. We develop a list of factors that should be taken into the account by NATO commanders when assessing and managing the risks of cyber operations.

A. Vertical Escalation in the Cyber Domain

The word escalation implies linear movement; up, maybe down, but never sideways. When applied to war or conflict, the metaphor is concise. A conflict at one level can move or be moved to the next higher—or, with de-escalation, lower—level. Given two levels of conflict, one is always and unambiguously higher than the other. Moving from one level to a higher level makes the level after that easier to reach, and therefore more likely. As a metaphor,

escalation is literally one-dimensional. From this metaphor come concepts such as escalation dominance, escalate-to-de-escalate, and de-escalation signalling.

This linear conceptualisation has dominated scholarly debate on escalation in the cyber domain. Adversaries climb escalation ladders by first engaging in strategic signalling of cyber defence capabilities and then exploiting each other's networks, perhaps culminating in attacks on critical infrastructure (Kostyuk, Powell & Skach, 2018; Lin, 2012). From a commander's perspective, escalation requires understanding the thresholds that trigger an adversary's decision to escalate or de-escalate. The thresholds that trigger a response may be obvious only to the other side. As with conventional domains, in cyberspace, this opens doors to the miscalculation of the adversary's reaction and unintended escalation. The conflicting parties may not share an understanding of how cyber attacks fit into the other side's escalation ladder. Such a misunderstanding of the adversary's intentions could be more likely in cyberspace because of the greater prominence of emotions and cognitive biases that affect perceptions and the choice of corresponding countermeasures (Manzo, 2011; McDermott, 2019; Kreps & Schneider, 2019; Tomz & Weeks, 2020).

1) Escalation Lattice: Scenarios
We contend that if the effects of cyberspace operations are consequential enough, then the notion of escalation as a ladder may be misleading. Rather, escalation may be more like a lattice allowing horizontal as well as vertical movement. In truth, escalation was never strictly a ladder, despite Herman Kahn's focus on the escalation ladder metaphor in his classic study, *On Escalation* (1965). Besides the more commonly understood concept of vertical escalation—a change in intensity—there sits horizontal escalation in which the conflict moves into other theatres or domains (e.g., from sea to land), or includes additional participants. Horizontal escalation of the 1962 Missile Crisis, for instance, would have occurred if the Soviet Union had put its own 'quarantine' around Berlin, which it did not.

For the most part, though, in the bipolar world for which modern concepts of escalation developed, escalation meant vertical escalation. The literature on horizontal escalation is scarce and focuses only on the conventional domains (Epstein, 1983; Fitzsimmons, 2019). To the best of our knowledge, there have been no previous attempts to examine the relevance of horizontal escalation to cyberspace. Such conceptualisation is long overdue because in a conflict involving significant cyber operations it may not be obvious that one outcome is at a higher level than another.

To illustrate the possible ambiguities introduced by cyberspace operations—and this applies at both the tactical and strategic levels—consider a few hypothetical scenarios.

One, NATO and Russia confront one another in the Baltic over Russian

attempts to expand its sea and air military exclusion zone around Kaliningrad. Each side is pouring naval and related air forces into the region: both are conducting operations in close proximity to one another. The situation is dangerous, not least because the next step appears to be a kinetic naval conflict. Russia (to pick one side) concludes that actual naval conflict would be a disaster but that it cannot give up the fight. So, while quietly withdrawing its naval forces from the stand-off, it launches devastating cyber attacks on the US homeland, aware that it could well suffer similar attacks from the US. Question: did it escalate or de-escalate?[1] The argument for a de-escalatory reading is based on the transition from potentially violent outcomes in the physical domains to costly but nonlethal outcomes in the virtual one. The case for an escalatory reading reflects the transition from regional, even off-shore conflict, to conflict against each side's homeland. Finally, whereas a naval confrontation or even combat can have a known endpoint because of the clear difference between war and peace, strategic cyber war may be harder to terminate because of attribution issues and the gauzy barrier between minor chronic and major acute cyber attacks.

Two, NATO is pushing back against the unprofessional and dangerous behaviour of Russian military jets in the Norwegian Sea. An incident occurs in which the ship of a NATO member nation has been damaged by an 'accidental' release of ordnance. In Brussels, leaders contemplate two options. One is to surge naval forces into the Norwegian Sea and alter the rules of engagement to raise the risk to Russian aircraft; the other is to initiate cyberspace and electronic warfare operations to suppress or at least confuse Russian surveillance capabilities during the confrontation. Which would be more escalatory? The first raises the risk of casualties. The second does not. But suppose Russian surveillance capabilities are suppressed and the Russians conclude it was due to cyberspace operations or Russia directly detects such cyberspace operations. If so, the Russians may well conclude that the purpose of such cyberspace operations is not limited to the confrontation at hand but is an attempt to blind Russian defences and lay the groundwork for a much broader set of NATO offensive kinetic operations. Worse; suppose further that these surveillance assets also serve as part of Russia's nuclear early-warning or command-and-control systems.

Three, after a tense standoff outside Narva (Estonia), Russian forces conspicuously withdraw several kilometres but at the same time, the volume of cyberspace intrusions into both civilian and military telecommunications that serve the border area appears to be rising. What is NATO to make of this? Is the crisis dissipating, as judged by the behaviour of Russian forces, or deepening due to the increased activity in cyberspace? If the Russians are using cyber attacks to create an opening for a raid-in-force, why are forces being demobilised? Could such behaviour—pulling forces back but ramping

[1] The question (albeit in a scenario involving China rather than Russia) was part of a final exam for Professor Libicki's students who had, a month earlier, participated in a war game with this scenario. Forty percent felt it was escalatory; sixty percent, de-escalatory. This split suggests the ambiguity is real.

up cyberspace operations—be like rolling dice and hoping for snake-eyes? Perhaps no single individual attempt to subvert NATO forces is likely to succeed and so continued mobilisation at the border is a waste of effort. But if one does succeed, it would be very useful to have forces nearby to exploit such an opening.

B. What, Exactly, Is Escalation?
There are many ways of assessing whether the transition from one state of conflict to another is escalatory. In a world in which escalation is one-dimensional, all the criteria would agree with one another: if A is more escalatory than B, it is more escalatory by every criterion that can be used to measure escalation. But, when escalation is multi-dimensional, A may be more escalatory than B by some measures and less by others, adding to the ambiguity.

Let us start with a basic definition of escalation as 'an increase in the intensity or scope of conflict that crosses a threshold(s) considered significant by one or more of the participants' (Morgan et al., 2008: p. 8). Metrics of intensity (vertical escalation) or scope (horizontal escalation) may or may not involve thresholds. The mutual escalation of both US and communist forces in South Vietnam *circa* 1965 was by degree—force levels rose on both sides. But they were not escalation by type: no consensus or even unilaterally declared threshold was crossed. Crossing a threshold implies a change in intensity, or at least opens the door to it. The atomic bombing of Hiroshima killed as many as the firebombing of Tokyo, but the former definitely crossed a threshold, albeit not one marked out in advance.

An additional helpful criterion that would apply whether or not escalation was a ladder or a lattice is whether the escalatory act is likely to be repeated or is, conversely, exemplary. The NotPetya cyber attack that caused roughly $10 billion of damage to the global economy in 2016-2017 but did not kill anyone clearly represented an increase in intensity, but nothing similar has taken place subsequently. If that trend continues, NotPetya, in retrospect, will have been less escalatory than a similar attack that would have been the first of many comparable cyber attacks. Russian DDoS attacks on Turkey in response to Turkey's 2015 downing of a Russian jet ended once the point was made. In retrospect, therefore, its cyberspace response could not be deemed escalatory: it did not set a new standard for conflict in that dyad.

If escalation is a ladder, this implies that every step up makes reaching higher steps more likely. In many ways, this is why escalation matters: the greater costs involved in going from one level of conflict to another are self-evident, but the greater risk that accompanies such a move needs a theory of escalation to be seen. This rule need not pertain to every individual step. Herman Kahn's treatment of escalation had 44 rungs, but he took care to state that no progression to all-out nuclear war would necessarily hit every step: skipping several at a time would be the rule. Nevertheless, the odds of reaching a nuclear Armageddon rose with each step up, as did the odds

of reaching or surpassing any intermediate state. Granted, in some cases escalation could be an exemplary act by one side to force a de-escalatory effect if it scared the other side into seeking terms 'escalate-to-de-escalate' (Work and Winnefeld quoted in Schneider, 2017). But analysts argue that Russia's tactical nuclear strategy is not to seek terms through escalation but through a credible threat to escalate (Oliker & Baklitskiy, 2018) and it is possible that, while the use of tactical nuclear weapons may increase the odds of coming to terms, it may also raise the odds of further escalation to strategic nuclear exchange. Stalemates can be resolved in more than one way.

If escalation is a lattice, increases in intensity, at least as measured by one metric, may not necessarily raise the odds of further escalation, particularly if measured by a different metric. Take the first scenario, in which strategic cyber war—a systematic set of cyber attacks aimed at the other side's society and economy rather than its military—began as a substitute for a potential naval engagement. Now compare each choice in terms of its *further* escalation potential. The 2018 US *Nuclear Posture Review* (DoD, 2018) and a 2013 Defense Science Board report (ibid, 2013) held out the possibility that a sufficiently grave cyber attack on the critical infrastructure *could* lead to nuclear retaliation, although it is difficult to see that taking place without there being many deaths directly resulting from such an event. More plausibly, such a cyber attack could lead to a kinetic retaliation on the perpetrator's homeland,[2] which, itself, might escalate to nuclear weapons use. But a kinetic naval confrontation carries its own risks, especially if the losing side feels pressure to up the ante to the use of nuclear weapons as a way of taking out many naval targets at once. There are other pathways: one might lead from naval engagements to attacks on ports and their infrastructures. These might then be considered attacks on the homeland, giving rise to conventional attacks on other homeland targets that support military operations, and thence to nuclear attacks.

With multiple escalation pathways, it is not obvious that increases in intensity correlate with increases in the odds of further escalation. This applies especially if one set of paths comes from an intensification of force-on-force engagements, and another entails attacks on each side's homeland. This further complicates the assessment of whether one state of conflict is more escalatory than another.

C. Implications for Risk Management

A shift from ladders to lattices would complicate escalation management by multiplying ambiguities and uncertainties, but these are not always bad. It is as easy to imagine new possibilities leading to escalation foresworn or to de-escalation as it is imagining it leading to further escalation. This complicates

[2] During the May 2019 conflict between Israel and Hamas in Gaza, Israel declared that it had struck a building housing hackers who had just targeted Israel. Note, however, that kinetic war was already ongoing at the time of the cyber attack; also, it is not obvious that the building would have gone unstruck were it not for the cyber attack (Borghard & Schneider, 2019; Chesney, 2019).

risk management because of a greater risk of unintended escalation. Certain features of cyberspace operations may create more ambiguity over what is or is not escalatory due to several factors.

First, it is harder to understand the adversary's intentions in cyberspace. Cyberspace operations can potentially affect kinetic operations at all levels of conflict. As in the second scenario above, an intrusion meant to confound low-level kinetic confrontations can also confound more intense conventional kinetic operations or, in some cases, nuclear operations. The target may not know the attacker's intentions. Perhaps the attacker meant to have local effects (as in the second scenario), but the target reacted as if the attacker sought global ones.

Interpreting intentions becomes even more complicated in the light of multiple escalation pathways that may confound the tacit agreements associated with escalation management. If one side foregoes the opportunity to attack objects or use weapons that would escalate a conflict, it often does so under the assumption that the other side would do likewise. If the other side cheats, so to speak, it gains an advantage and makes the first look weak, which thereafter has less reason to restrain itself. Consider a situation in which neither side had previously escalated in a particular direction but then one side escalates in cyberspace. The other side could ignore it but would probably feel both pressured and entitled to react. It would ask itself whether the tacit agreement not to escalate in any domain was still in effect. If it determines that one direction—say, a cyberspace operation—is different from the traditional direction, it may well deem that the tacit agreement held in the kinetic arena and respond only in cyberspace. This tendency to treat cyberspace escalation as different in type from kinetic escalation would be reinforced if there were no tacit agreements in cyberspace that the cyberspace operation broke. This proposition is not absurd; many cyberspace operations are not only tactical but strategic surprises, in that the victim may not have believed that the attacker was interested in or allowed itself to carry out a particular operation. Conversely, the other side may deem any escalation in whatever medium a violation of the tacit accord and respond in whatever medium most favours it. One of the problems with a tacit agreement is its terms are never defined and hence each side may interpret what has been 'agreed' differently.

A further confounding variable merits note: is it the effort made, or the effect produced that marks escalation and indicates that a tacit agreement has been broken? This is relevant in cyberspace where most failing efforts fail quietly, while only those with effect are detected. Catching the other side trying to violate the agreement is evidence of bad intent and shows that the tacit agreement is no longer a constraint on the other side but, particularly in cyberspace, detecting an attempt in progress does not always indicate what the intention was and may not have left enough clues for positive attribution. In the physical world at least, the fact of failure makes a difference—the current US Administration has made a point of not responding to failed

North Korean missile launches (Fifield, 2017). In contrast, Israel responded with a cyber attack on one of Iran's ports in retaliation for unsuccessful cyber attacks on Israeli waterworks (Bergman & Halbfinger, 2020; Warrick & Nakashima, 2020).

Second, thresholds for escalation are more ambiguous in cyberspace. Compared to low-level violent conflict, cyberspace operations can be far costlier in time and therefore money. The bill for the many depredations of the 2017 NotPetya attack was roughly $10 billion. Yet, cyber attacks are rarely destructive and have not thus far killed anyone directly. To economists who routinely put a monetary cost on life in making cost-benefit calculations, many cyber attacks are more serious than military confrontations short of fully committed war. An ethicist who believes that the individual life is priceless such as Immanuel Kant would consequently draw a line between lethal and nonlethal operations that clearly put the use of lethal force above the line and cyber attacks, however costly, below it. This makes it more difficult to predict an adversary's thresholds for escalation. Will an attack on the electricity grid trigger the same reaction as an attack on financial institutions?

Despite the unending confrontations in cyberspace, strategic cyber war's potential to wreak serious damage on a modern economy is still a matter of dispute. The closest analogue may come from Russia's assaults on the Ukrainian economy. However, narratives about that conflict still focus on the loss of lives and territory brought by war and not the day-to-day difficulties associated with constantly losing online services because information systems have failed. The more consequential a strategic cyber war offensive, the more escalatory its introduction would be. The harder it is to guess its impact in advance, though, the greater the disagreement in assessing whether the start of such operations is escalatory.

The role of psychological effects is an additional factor that complicates the calculation of the desired effects. Even when cyber operations do not impose high economic costs, they might be perceived by state-actors as humiliating and trigger a disproportionate reaction to restore national dignity and regain trust in the eyes of the electorate. Emotions can trigger a response that by far outweighs the extent of economic costs.

Third, having multiple escalation paths obfuscates the de-escalation process. One possibility, alluded to above, arises from the fact that cyber war is understood differently by different parties. The media hypes the threat.[3] To war fighters, the disruption of cyber war is often just something else that could go wrong in an environment where things go wrong all the time. This disjunction allows a narrative in which one side's leaders trumpet their unsheathing of a bold new weapon as an indicator that they are still in the fight, but on the other side, cyber war adds complication but not necessarily catastrophe. Countries can thus mask their unwillingness to march to a confrontation by

[3] Consider the 3 July 2010 cover of the normally sober Economist which (unironically) uses a picture of a nuclear explosion as a metaphor for cyber war.

starting a new, albeit less lethal, one in cyberspace. But this option is not free. Because of delayed effects, potential rogue players and attribution issues, it may be more difficult to cleanly terminate a cyber war than to end its kinetic equivalent. It may trade an acute crisis for a chronic headache without a clear path to termination.

De-escalation would also look different if it were less like climbing down a ladder and more like working one's way down a lattice. But the difficulties may not echo those of escalation. Escalation and de-escalation are not opposite actions: the milestones on the road up rarely match those on the way down. In some cases, escalation may be publicised as a way of brandishing a capability or signalling a commitment: escalate to de-escalate. In other cases, escalation could be stealthy, to gain an advantage without sparking the other side to do likewise and thereby nullify the advantage. By contrast, de-escalation, withdrawal, is often a choice to temporarily yield an advantage to persuade the other side to impose constraints on itself; it must be effectively communicated if it is to do that. Given the tendency for parties in conflict to make worst-case assumptions about each other, one can expect that signs and portents of escalation would be eagerly seized upon as evidence of the other side's bad faith and intentions; inadvertent escalation is a serious concern in international relations (Posen, 1982). But the opposite is not so common. One side may eagerly await signs that the other is backing off[4] but, otherwise, may be suspicious of signals of de-escalation. A signal may be a mind game or a Trojan horse.

The ambiguities of cyberspace would hardly allay such suspicions; more likely they would exacerbate them. Consider one side that would signal de-escalation by ceasing cyber attacks. So, the other side stops seeing them. What would explain a fall-off in sightings? A confidence-building measure by the other side? A hiatus while other targets are being prepared? Evidence that its own defences are working better? If the other side counted all detected intrusions as potential cyber attacks, would a decrease in detections be considered a signal or evidence that the other side's cyberspace operations were now stealthier, or that its own ability to detect such operations has been compromised?

Any move to signal de-escalation by *substituting* cyberspace operations for kinetic operations confronts the possibility of more misinterpretation, as it assumes that both sides understand one to be less painful and less consequential than the other. But such understanding may be one-sided. Worse, events, such as a cyber attack on an infrastructure that yields indirect effects much costlier than their direct effects may turn the narrative around. If homeland cyber attacks are deemed more dangerous than some faraway kinetic conflict, something that one side thought signalled de-escalation would be read very differently.

[4] Consider the delusionary search for peace feelers for the Vietnam War in the later Johnson administration.

Fourth, the existence of multiple escalation pathways also complicates escalation dominance. Such a strategy requires one side to demonstrate that no escalated level of conflict would make the other side better off; a more muscular version is that one side will 'dominate' at every escalated level of conflict. But the greater the number of paths upward, the greater the burden on those seeking escalation dominance. They have to cover more bets. Conversely, demonstrating dominance only along costly escalation paths may, as above, create options for the other side to exploit escalation paths that call attention to themselves but are not particularly costly either as such or to the overall war effort. In other words, the existence of multiple pathways permits tolerable outcomes by channelling conflict in less damaging paths rather than having to suppress it entirely.

D. Implications for NATO's Operations in Cyberspace

At the Warsaw Summit, the Allies agreed to develop capabilities to operate in cyberspace 'as effectively as ... in the air, on land, and at sea' and to strengthen and to support the Alliance's overall deterrence and defence posture (NATO, 2016:§70). Our analysis calls into question whether the efficiency of cyber operations could be compared using the same metric used for kinetic options because of the inherent ambiguity with regards to its escalatory and de-escalatory effects. When escalation proceeds in a nonlinear manner, commanders should assess the effects beyond the threshold at which cyber capabilities are used. Even though both cyber and kinetic options could generate similar immediate tactical effects, for example by piercing an Anti-Access/Area Denial (A2/AD) bubble, the strategic implications of using cyber capabilities are more ambiguous and harder to predict. By widening the conflict to multiple domains, NATO could obscure its hand regarding the next move and exploit this ambiguity to gain tactical and operational advantage. Conversely, it also implies that NATO commanders could also misread the intentions of an adversary in the cyber domain. The conceptual shift from ladders to lattices that comes from considering the role of efficacious cyberspace operations in a crisis or conflict would, not surprisingly, complicate escalation management. Likewise, it introduces ambiguities and uncertainties.

This also implies that risk management in cyberspace requires developing in-house expertise not only of adversary's technological vulnerabilities, but also of threat perceptions, corresponding thresholds and political constraints that can influence subsequent responses. It entails greater Human Intelligence and open-source intelligence sharing among Allies whenever cyberspace effects are being sought. This also requires more refined scenario development for NATO exercises. Its goals would be to assess the technological capabilities available to achieve the cyberspace effects and understand how the use of such capabilities may appear to relevant actors.

2. CONCLUSIONS

It is difficult enough to determine the degree of escalation in a confrontation involving only cyberspace operations. Once other elements of power are also involved, comparisons between the real and the virtual can yield different conclusions from different perspectives. The challenges to NATO are not entirely virtual; as there are real-world elements ranging from unidentified combatants (sometimes known as little green men), proxy warriors and unprofessional military activities to the brandishing of nuclear weapons. So, comparisons—is *this* worse than *that*—are inevitable.

The difficulty of determining whether shifts in a confrontation towards cyberspace are or are not escalatory is of a piece with the many ambiguities of this newest domain of conflict. If NATO aims to 'win' any possible confrontation with its opponents, regardless of where it leads, labelling any one development as being escalatory is secondary. But if NATO wants to manage these confrontations and settle them at modest cost and risk to the Alliance's values, then correct understandings of escalation begin to matter.

NATO faces several paths. One is to de-emphasise signalling altogether and accept that modern confrontations will be too ambiguous and noisy for one side's implications (or even statements) to translate with fidelity into the other side's inferences. Russia will reach its own conclusions about NATO regardless of what NATO tries to convey, especially when through wordless deeds. The other is to use dialogue to help build a foundation for evaluating and responding to the evolution of confrontations. A great deal of the ambiguity in evaluating cyberspace operations is inherent in the medium itself, so dialogue may not guarantee that all such shifts and signals garner the correct response. Yet, it may narrow the range of plausible responses and reduce the occurrence of nonlinear reactions that lend unnecessary instability to such confrontations.

3. REFERENCES

Bergman, R. & Halbfinger, D. M. (2020) Israel hack of Iran port is latest salvo in exchange of cyberattacks. *The New York Times*. 20th May. Available from: https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html [Accessed 12th July 2020].

Borghard, E. D. & Schneider, J. (2019) Israel responded to a Hamas cyberattack with an airstrike. That's not such a big deal. *The Washington Post*. 9th May. Available from: https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/ [Accessed 21st September 2020].

Chesney, R. (2019) Crossing a cyber Rubicon? Overreactions to the IDF's strike on the Hamas cyber facility. *Lawfareblog.com*. 6th May. Available from: https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility [Accessed 21st September 2020].

Epstein, J. M. (1983) Horizontal escalation: sour notes of a recurrent theme. *International Security*. 8 (3), 19-31. Available from: http://www.jstor.com/stable/2538698 [Accessed 10th July 2020].

Fifield, A. (2017) U.S. says it ignored North Korea's latest missile launch because it failed; VP Pence arrives in Seoul. *National Post.* 16th April. Available from: http://news.nationalpost.com/news/world/u-s-ignores-north-koreas-latest-missile-launch-because-it-failed-as-vice-president-heads-to-asia [Accessed 2nd June 2020].

Fitzsimmons, M. (2019) Horizontal escalation: an asymmetric approach to Russian aggression? *Strategic Studies Quarterly*. 13 (1), 95-113. Available from: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-1/Fitzsimmons.pdf [Accessed 7th July 2020].

Kahn, H. (1965) *On Escalation: Scenarios and Metaphors.* New York, NY, Praeger.

Kostyuk, N., Powell, S. & Skach, M. (2018) Determinants of the cyber escalation ladder. *The Cyber Defense Review*. 3 (1), 123-134. Available from: https://www.jstor.org/stable/26427380 [Accessed 20th June 2020].

Kreps, S. & Schneider, J. (2019) Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics. *Journal of Cybersecurity*. 5 (1), 1-11.Available from: https://doi.org/10.1093/cybsec/tyz007.

Lin, H. (2012) Escalation dynamics and conflict termination in cyberspace. *Strategic Studies Quarterly*. 6 (3), 46-70. Available from: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-3/Lin.pdf [Accessed 8th August 2020].

Manzo, V. (2011) Deterrence and escalation in cross-domain operations: where do space and cyberspace fit? *Strategic Forum*. 272, 1-8. Available from: https://www.questia.com/library/journal/1G1-291503426/deterrence-and-escalation-in-cross-domain-operations [Accessed 13th July 2020].

McDermott, R. (2019) Some emotional considerations in cyber conflict. *Journal of Cyber Policy*. 4 (3), 309-325.

Morgan, F.E., Mueller, K.P., Medeiros, E.S., Pollpeter, K.L. & Cliff, R. (2008) *Dangerous Thresholds: Managing Escalation in the 21st Century*. Santa Monica, CA, Rand Corporation.

NATO (2016) Warsaw Summit Communiqué. 9th July. Available from: https://www.nato.int/cps/en/natohq/official_texts_133169.htm [Accessed 24th October 2020].

NATO (2020) *AJP-3.20: Allied Joint Doctrine for Cyberspace Operations*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf [Accessed 21st July 2020].

Oliker, O. & Baklitskiy, A. (2018) The nuclear posture review and Russian 'de-escalation:' a dangerous solution to a non-existent problem. *War on the Rocks*. 20th February. Available from: https://warontherocks.com/2018/02/nuclear-posture-review-russian-de-escalation-dangerous-solutionnonexistent-problem/ [Accessed 8th August 2020].

Posen, B.R. (1982) Inadvertent nuclear war? escalation and NATO's northern flank. *International Security*. 7 (2), 28–54.

Schneider, M. B. (2017) Escalate to de-escalate. *Naval Institute Proceedings*. 143/2/1368. February. Available from: https://www.usni.org/magazines/proceedings/2017/february/escalate-de-escalate [Accessed 21st September, 2020].

Shea, J. (2017) How is NATO meeting the challenge in cyberspace. *Prism*. 7 (2), 18-29. Available from: https://apps.dtic.mil/dtic/tr/fulltext/u2/1044679.pdf [Accessed 14th July 2020].

Smeets, M. (2019). NATO member's organizational path towards conducting offensive cyber operations: a framework for analysis. In : Minárik, T., Alatalu, S., Biondi, S., Signoretti, M., Tolga, I., and Visky, G. (eds.) *2019 11th International Conference on Cyber Conflict: Silent Battle*, 28-31 May 2019, Tallinn, Estonia. NATO CCDCOE Publications. pp. 1-15. Available from: doi:10.23919/CYCON.2019.8756634.

Tomz M. & Weeks, J. LP. (2020) Public opinion and foreign electoral intervention. To be published in *American Political Science Review*. [Preprint] Available from: https://iriss.stanford.edu/sites/g/files/sbiybj6196/f/publications/public_opinion_and_foreign_electoral_intervention.pdf [Accessed 1st June 2020].

U.S. Department of Defense (2013) Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. January. Available from: https://dsb.cto.mil/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf [Accessed 21st September 2020].

U.S. Department of Defense (2018) Nuclear Posture Review. February. Available from: https://dod.defense.gov/News/SpecialReports/2018NuclearPostureReview.aspx [Accessed 21st September 2020].

Warrick, J. & Nakashima, E. (2020) Officials: Israel linked to a disruptive cyberattack on Iranian port facility. *The Washington Post*. 18th May. Available from: https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html [Accessed 18th May 2020].

PART II:
New Technologies and NATO's Response

Securing 5G: NATO's Role in Collaborative Risk Assessment and Mitigation

Luiz A. DaSilva
Bradley Professor of Cybersecurity and Executive Director
Commonwealth Cyber Initiative
Virginia Tech

Jeffrey H. Reed
Willis G. Worcester Professor
Bradley Department of Electrical and Computer Engineering
Virginia Tech

Sachin Shetty
Associate Director and Associate Professor
Virginia Modeling, Analysis, and Simulation Center
Old Dominion University

Jerry Park
Professor
Bradley Department of Electrical and Computer Engineering
Virginia Tech

Duminda Wijesekera
Professor
Computer Science
George Mason University

Haining Wang
Professor
Bradley Department of Electrical and Computer Engineering
Virginia Tech

Abstract: The 5th generation of mobile systems (5G) unleashes a new cohort of services that promise to revolutionise transportation, manufacturing, and healthcare and to have a major economic impact. 5G systems are also being adopted by military organisations. They introduce a unique set of security challenges related to the trend towards a 'softwarisation' of the network, the support for high-reliability services, and the international supply chain for these networks. This paper outlines measures that governments, and in par-

ticular the NATO Alliance, should put in place for risk assessment and the certification of secure 5G components and systems. We also make the case for NATO's coordination and support for enhanced international collaboration through articulating a common 5G strategy that informs participation in the standardisation process and public-private partnerships to maintain databases of security threats and their mitigation.

Keywords: *5G, cyber security, virtualisation, certification, standards, public-private partnership*

1. INTRODUCTION

If any doubt remained about communication networks making up a key component of our critical infrastructure, the COVID-19 crisis has put it to rest. With the increased role that these networks play in keeping the economy going, new threats have emerged and existing ones intensified. For example, the healthcare industry has been experiencing a surge in ransomware attacks, with an increase of 350 per cent reported for the last quarter of 2019, a trend that has only worsened in 2020 (Corvus Insurance, 2020). With 5G networks starting to be deployed worldwide, there is justified concern about new cyber threats associated with this technology.

The introduction of any network technology creates the potential for new security attacks, but in some respects 5G is different. It builds on previous generations of cellular technology by improving the bandwidth, capacity, latency and reliability of mobile broadband services. With its promise to enable a new generation of services through ultra-reliable low-latency communications, 5G can also significantly expand the attack surface of the network (Frost and Sullivan, 2020). If applications such as smart homes and blended autonomous vehicles depend on 5G, an attack on the network can have safety-of-life consequences. The apparent dominance of Chinese vendors in the 5G space has also raised questions in the US and elsewhere about the level of independence of vendors from national governments (Iplytics, 2019).

Addressing both technical and geopolitical challenges in 5G security will require strong international cooperation that goes beyond the standardisation process that already takes place in the 3rd Generation Partnership Project (3GPP) and other standards bodies. We believe that this must include the development of international benchmarks for 5G security and a certification process for hardware and software to pass stringent security tests. Recent strides in artificial intelligence can be leveraged for the creation of automated tools to check for security vulnerabilities.

The core principles for 5G security can benefit strongly from international consensus and NATO member states can have a role in establishing the mechanisms for this consensus to emerge. Relevant metrics should be identified and tracked through an international 5G cyber security-focused Infor-

mation Sharing and Analysis Centre (ISAC). An open vulnerabilities database should be created, thereby increasing transparency and affording industry, government and academic stakeholders access to shared information on those security threats plaguing the 5G infrastructure.

The geopolitical issues in the supply chain for 5G networks also require a coordinated approach. The open radio access network concept and, more broadly, the reliance upon 5G systems that are open by design, will encourage the disaggregation of those software and hardware ecosystems associated with 5G. This process has the potential to mitigate the threat posed by supply chain attacks and promote a diversification of 5G vendors.

The broad problem of cyber security in 5G can only be handled adequately through coordination between researchers, industry and policymakers from across the globe. With the strategic role that 5G is starting to play in national security and military organisations, NATO is well placed to facilitate this coordination. This article summarises unique security aspects brought about by the advent of 5G and presents recommendations for how the international community and NATO, in particular, can respond to these challenges.

2. 5G SECURITY: WHAT'S NEW?

The vision for 5G security includes security by design, flexibility to respond to new threats, and automated security systems leveraging artificial intelligence (Ahmad et al., 2019). The International Telecommunication Unit Telecommunication Standardisation Sector (ITU-T) has a number of study groups involved in drafting security standards and recommendations. These efforts are complemented by those of other international standardisation bodies such as the 3GPP, the European Telecommunications Standards Institute (ETSI) and the Internet Engineering Task Force (IETF).

Nevertheless, some unique concerns attach to the issue of security in 5G systems: a) the virtualisation of network functions and resources; b) the 5G pillars of massive machine-type and ultra-reliable, low-latency communications (Sexton et al., 2017); and c) concerns about the international supply chain for 5G equipment. These are summarised in Figure I.

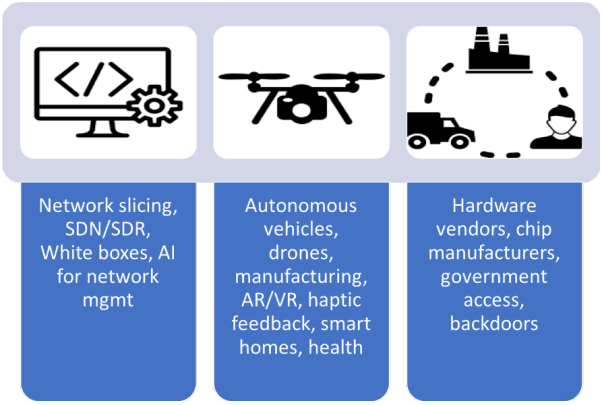
First, softwarisation—that is, moving functionality that was traditionally provided in hardware to software—is a major trend in networks with the advent of Software Defined Network (SDN) and Software Defined Radio (SDR) and the replacement of network-specific hardware with white boxes. In 5G, this trend gains additional steam through a concept called slicing. Network virtualisation and slicing techniques enable the running of multiple logical networks as independent business operations on a common physical infrastructure (Afolabi et al., 2018). In essence, each network slice represents an independent virtualised end-to-end network and allows operators to deploy multiple services with distinct architectures in parallel over the same physical network. While virtualisation and slicing play a critical role in 5G systems,

they also introduce potential security vulnerabilities due to the challenge of simultaneously providing strong resource isolation and efficient resource use in a virtualised environment. Exploiting the shared physical platforms in 5G infrastructure, adversaries could construct side channels or covert channels to impose serious security threats on 5G communications. Thus, it is essential to protect the slice-provisioning process in 5G infrastructures against malicious attacks and to ensure strong slice isolation.

Second, the specifications for 5G are built on three pillars: enhanced mobile broadband; Massive Machine Type Communications (MMTC); and Ultra-Reliable Low Latency (URLL) communications. The last two present a paradigm shift for wireless networks in terms of the need to scale massively (in the case of MMTC) and in the support of stringent reliability requirements (for URLL). They also expand the attack surface of the network to a new class of devices—sensors and Cyber Physical Systems (CPSs)—and services from autonomous transportation to Augmented and Virtual Reality (AR/VR). Attacks on those services can present safety-of-life risks: imagine, for example, a hacker taking control of an autonomous vehicle.

The third area of specific concern in 5G relates to the reliability and trustworthiness of the supply chain for those networks. Huawei Technologies currently leads in the number of declared 5G patent families (Iplytics, 2019), followed by Samsung and LG Electronics. Among the top ten companies in this category, only two are based in Europe (Nokia and Ericsson, in fourth and sixth positions, respectively) and two in the US (Qualcomm and Intel, in seventh and eighth, respectively). The geopolitics of 5G have dominated the news of late, with the US exerting pressure on its allies to not deploy 5G testbeds based on Huawei equipment. Concerns are around a close relationship between the vendor and the Chinese government, with the potential for privacy and security violations (Kaska et al., 2019).

Figure I. Unique aspects of 5G security include issues related to softwarisation (left), high-reliability services (centre) and the supply chain (right).



The softwarisation and virtualisation of 5G, including the introduction of service orientation in the 5G ecosystem, bring advantages and disadvantages. The 5G architecture introduces mobile edge computing (Liu et al., 2018; Mao et al., 2017) as a key component of its architecture that will enable faster and diverse services for new use-cases such as e-health or connected autonomous vehicles. However, virtualised service-oriented architectures have a long history of vulnerabilities (Riaz & Tahir, 2018; Tank et al., 2019), kill chains (Kim et al., 2019; MITRE, 2020) and post-attack forensics (Sharevski, 2018). In addition, the newer application domains may connect their specialised equipment and controllers to 5G base stations. This makes vulnerability tracking and associated risk evaluation and post-attack forensic examinations more complex and issues such as supply chain security and attack attribution more challenging.

The deployment of 5G services will involve re-architecting the wireless cellular network with new capabilities such as software-defined networking, network function virtualisation and a cloud-native architecture. These enhancements bring the need for cyber defence in the edge, secure network slicing, secure multi-access edge computing and access control policies for a disaggregated radio access network.

In the next two sections, we propose a number of actions that can be taken to address these challenges and how NATO, together with the broader international community, can establish tighter collaboration in identifying and overcoming the security threats that may arise with this new technology.

3. RISK ASSESSMENT AND MITIGATION

The adoption of 5G poses several security risks that not only affect commercial services but may also have national security implications. In this section, we discuss the need for the development of risk assessment techniques, certification and regulation of 5G equipment and networks.

A. Risk Assessment and Mitigations Efforts in the US

To date, academic researchers who have studied security risks associated with 5G adoption have focused on assessing the security vulnerabilities in the 5G network protocol or security issues germane to its core functionalities (Cremers & Dehnel-Wild, 2019; Hussain et al., 2019; Jover & Marojevic, 2019). The scope of those works is somewhat narrow, as they focus exclusively on technology-centric issues. For example, Jover and Marojevic (2019) focus on vulnerabilities in the 5G Radio Access Network (RAN) security architecture and procedures, while Hussain et al. (2019) use formal methods to analyse a simplified 5G protocol model covering six key control-layer protocols.

Recently, government agencies of a number of countries including the US and European Union (EU) member states have released reports and white papers that describe their 5G strategy and risk assessment of 5G security and propose strategies for mitigating those risks (CISA, 2019; DoD, 2020; European Commission, 2020; NIS Cooperation Group, 2019, 2020; White

House, 2020). In contrast to the academic literature, these reports take a much broader view in assessing the risks associated with 5G adoption, with a particular emphasis on supply chain vulnerabilities and the risks associated with untrusted 5G equipment vendors.

In particular, the Cybersecurity and Infrastructure Security Agency (CISA) of the US's Department of Homeland Security (DHS) published a note that represents an analysis of the vulnerabilities in the supply chain, network security, deployment of 5G and the lack of diversity of 5G vendors in the market (CISA, 2019), pointing to:

- Supply chain vulnerabilities. Use of 5G components produced by untrusted vendors could expose these networks to vulnerabilities introduced by malicious hardware and software, counterfeit components and flawed components due to substandard manufacturing processes and maintenance procedures. 5G software, hardware and services provided by untrusted entities could also increase the risk of compromise to the confidentiality, integrity and availability of information sent and received over 5G networks.
- Network security vulnerabilities. Some aspects of 5G are based on enhancements to prior generation cellular technologies and most initial 5G deployments will use some components of the legacy 4G LTE infrastructure, as in the 5G non-standalone deployment model. These factors may expose 5G networks to some of the vulnerabilities of legacy systems. 5G may also have unknown vulnerabilities despite its security enhancements.
- Deployment vulnerabilities. Compared to previous-generation cellular technologies, 5G is more complex and is composed of many heterogeneous components that can provide additional attack vectors and surfaces. The efficacy of 5G's security enhancements will partially depend on proper implementation, configuration and deployment of those enhancements.
- Reduction of competition and trusted options. The domination of the 5G equipment and component market by a very small number of vendors increases the likelihood of proprietary 5G technologies proliferating in the market. Proprietary technologies that do not meet interoperability standards would be difficult to upgrade, repair and replace. This may increase the lifecycle cost of 5G equipment and infrastructure and may contribute to delays in 5G deployment. Limited interoperability among 5G technologies would harm competition in the market, raising barriers to the entry of smaller vendors.

B. Risk Assessment and Mitigation Efforts in the EU

In 2019, the EU published a report entitled EU coordinated risk assessment of the cyber security of 5G networks (NIS Cooperation Group, 2019) which follows the systematic approach dictated by an international standard on information security risk management, ISO/IEC 27005. The risk assessment described in the report is modelled on assumptions about use-cases

and plausible scenarios. Specifically, this risk assessment focuses on threat vectors; types of threats posed to 5G networks; assets and their degree of sensitivity; vulnerabilities; and risks and relevant scenarios.

The EU coordinated risk assessment report concludes that the cyber security challenges and threats related to the rollout and operation of 5G networks create a new security paradigm, which necessitates the reassessment of current security policies and frameworks. These challenges include, but are not limited to, the following issues:

- 5G networks' increased reliance on software-based virtualised network functions may result in increased exposure to attacks and additional potential entry points for attackers. The softwarisation of the network functions could also make it easier for threat actors to insert backdoors and other attack enablers into products and make them more difficult to detect.
- The network operators' increased reliance on a small number of 5G equipment vendors may increase exposure to security risks. This may also lead to a greater number of attack paths exploited by state-backed attackers, posing a threat to national security.
- To mitigate the threat posed by the increased exposure to attacks facilitated by equipment vendors, the creation of a risk profile of each equipment vendor may be necessary. This profile includes an analysis of the likelihood that the vendor is subject to influence by an adversarial country.
- A major dependency on one or two vendors significantly increases exposure to a myriad of availability and cyber security problems, including potential equipment supply interruption, service disruptions due to design flaws, bugs and vulnerabilities in the equipment hardware and software and possible exploitation of vulnerabilities by threat actors. Major dependency on a vendor with a high degree of risk presents an especially serious security issue.
- The unique attributes of the 5G network architecture and its novel functionalities may increase exposure to certain types of attacks or provide targets for cyber attacks. Management and Orchestration (MANO), which is a key element of a 5G core network's Network Function Virtualisation (NFV) architecture, may provide a tempting target for threat actors who intend to disrupt the services provided by a 5G core network.
- In addition to the traditional security concerns of confidentiality and privacy, threats to the availability and integrity of 5G networks will increasingly pose a significant risk. Unlike prior-generation cellular technologies, 5G networks are expected to enable and support a broad range of commercial and military uses, including smart factories, the Internet of Things (IoT), autonomous vehicles, AR/VR in military training and smart military warehouses. The integrity and availability of those uses will become major national security concerns.

4. CERTIFICATION AND VALIDATION

Most governmental regulatory authorities that regulate radio frequency (RF) communications, such as the Federal Communications Commission (FCC) in the US, carry out or oversee a programme to certify that RF-signal-emitting devices are compliant with rules and regulations and do not interfere with existing devices and systems that use their nation's airwaves. Under the direct guidance of regulatory authorities or guided by their regulatory constructs, the industry self-certifies wireless devices in a cost-effective, regulation-compliant manner, often by employing a process that is baked into their production and distribution processes.

Not surprisingly, the conformance testing and certification processes for 5G are extensive and international, as 5G is a set of truly global technologies. There are three types of entities involved in these processes: standards-setting entities, device-certification entities and regulatory entities. Specifically, for 5G testing and certification processes, the 3GPP sets the related standards, the Global Certification Forum (GCF) and the Personal Communications Service (PCS) Type Certification Review Board (PTCRB) mandate 3GPP test cases used for device certification and regulatory agencies around the globe such as the FCC issue regulations to ensure compliance. Test cases defined in 3GPP specifications are verified by using executable scripts. 5G chipset and device manufacturers must comply with the 3GPP test cases that the GCF and PTCRB have mandated to achieve certification. After the test cases are selected by the GCF and PTCRB, the test vendors implement the corresponding test specifications in their conformance test solutions.

At present, there are no systematic conformance testing and certification processes specifically aimed at 5G security. However, the cyber security certification programme for cellular-connected IoT devices (CTIA Certification, 2020) launched by the Cellular Telecommunications Industry Association (CTIA) has obvious relevance to 5G security. By offering cyber security certification for IoT devices, this certification programme aims to protect consumers and wireless infrastructure while creating a secure foundation for IoT use, such as smart cities, smart factories, connected automobiles and e-health. The programme builds on the IoT security recommendations from the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA). Multiple stakeholders, including leading mobile operators, device and equipment vendors, security experts and test labs were involved in the development of the programme's test requirements and plans.

These certification initiatives focus primarily on end-user devices. It is important to establish certification mechanisms for equipment deployed in the core and radio access networks. The EU cyber security certification framework for ICT products, devices and processes, established in the EU Cybersecurity Act (European Union, 2019) may serve as a starting point and can be extended to directly address 5G supply chain risks.

Due to several factors—including increased complexity, inherent heterogeneity and the softwarisation and virtualisation of critical functions—5G is expected to be more exposed to vulnerabilities and cyber attacks than its predecessors. To ensure the long-term success of 5G, it will be critical to certify that its devices and infrastructure are well protected from potential cyber attacks launched by threat actors under various scenarios. The first step in this direction is the establishment of a conformance and certification programme that specifically addresses security issues in 5G devices and systems. Such a programme should involve all relevant 5G stakeholders and follow well-established recommendations and procedures from regulatory agencies and global certification entities.

5. RECOMMENDATIONS FOR NATO'S SUPPORT TO GLOBAL 5G SECURITY COOPERATION

A. International Partnership for Risk Assessment and Product Testing

Countries must conduct a risk assessment of their security processes and adopt advanced security measures to ensure the successful deployment of 5G. A consortium of NATO nations and its strategic partners working together to develop cyber risk management policies for 5G systems is paramount. For example, the EU toolbox for 5G security (NIS Cooperation Group, 2020) has provided member states with the opportunity to conduct a gap analysis and launch new initiatives to improve existing security measures and enforcement mechanisms. The toolbox has aided a systematic self-assessment and has resulted in several member states being prepared to adopt advanced security measures on 5G cyber security. This initiative should be expanded to and adopted by non-EU NATO nations.

NATO and the Allies must each develop a strategy to ensure security by design for 5G beyond infrastructure deployment. This should include a rigorous process for vetting vendors and carriers of such networks. This process should be laid out by an international consortium of industry and government stakeholders, including the NATO Standardization Office (NSO) and other entities such as relevant Centres for Excellence that would look at balancing risk mitigation and security. The consortium should explore approaches to establishing and maintaining situational awareness over 5G supply chains and security practices of suppliers and vendors. This organisation would ensure that 5G products comply with security specifications provided by the 3GPP and other key standardisation bodies. It should also develop a framework for assessment, mitigation and management of the range of risks to 5G networks. This includes developing testing tools for automated evaluation of the security of 5G networks; artificial intelligence solutions that rely on shared data are promising candidates for this. Finally, the consortium should incentivise improvements in security with initiatives such as (i) easy access to license-free or lightly-licensed spectrum to incentivise innovation: (ii) incentives for shared accountability in the supply chain that results in access to trustworthy hardware and software: and (iii) investigation of new busi-

ness models that incentivise manufacturers and operators that meet security benchmarks.

As industries race towards deploying 5G networks in operational settings, there is a need to conduct a security analysis of the 5G infrastructure in diverse domain areas. Universities can play a key role in conducting security risk assessments with the potential to uncover exploitable vulnerabilities that could affect the resilience of the 5G infrastructure. Collaboration between research groups in North American and European universities can lead to an international research testbed on which to conduct empirical validation of innovative security technologies.

B. Cyber Threat Intelligence Sharing

5G security cannot be under the exclusive purview of technical teams. When a cyber threat emerges, it is generally detected first by private actors or by the public. Therefore, for organisations to be swift in responding to a cyber threat requires the fast sharing of relevant information by those actors. This can be accomplished through an Information Sharing and Analysis Centre (ISAC) (ENISA, 2018). The problem is thus to develop a cyber-threat information sharing capability allowing authorised participants to share real-time Cyber Threat Information (CTI) within an ISAC. That capability also has to ensure trust, anonymity and security to all users both inside and outside the ISAC. The significance of cyber security information sharing has led governments and regulators to mandate or encourage such sharing.

In the US, the Cybersecurity Information Sharing Act (US Congress, 2015) incentivises collaborative sharing among private- and public-sector organisations by providing liability protection to the sharing parties. The EU has also launched several cross- and intra-sector initiatives to enhance member states' capability for preparedness, cooperation, information exchange, coordination and response to cyber threats. ITU-T recommendation X.1215 also discusses how structured threat information expression (STIX) language can be used to support CTI and information sharing, such as knowledge of threats, vulnerabilities, incidents, risks and mitigations and their associated remedies (ITU-T, 2019). To ensure a successful CTI capability, there is also a need for a large number of participants who actively share cyber incidents. Limited participation in this information sharing can significantly impair the ability to manage cyber risks. For example, the DHS has reported that the limited number of participants that ingest cyber threat information is the main barrier to improving the quality of indicators that can provide actionable information to remediate cyber threats (Office of the Inspector General of the Intelligence Community, 2019).

The fundamental concerns of low participation in CTI sharing include lack of trustworthiness from the participating organisations, uncertain authenticity of the exchanged information, improper anonymity, the existence of free-riders, malicious insiders and the possibility of information tampering. Blockchain technology should be investigated for its potential for transparent

and trusted information exchange that would give provenance for vendors' and suppliers' actions. An example of blockchain's use for information sharing has been demonstrated by IBM's Mission Partner Environment (MPE) (IBM, 2018). The MPE is empowered by blockchain private channels that allow the exchange of unclassified information between unclassified and classified networks. The MPE facilitates multinational information sharing and ensures the number and size of each shared MPE are essentially reduced to ledger. The shared private channel ledger capability lowers implementation costs through the reuse of existing MPE resources, increases sharing by enabling countries to use their indigenous technologies and provides accountability via immutable ledger and fine-grained lifecycle security control.

C. Expansion of Standardisation to the 5G Ecosystem

There will be a need for several standardisation efforts focused on secure 5G infrastructure and secure 5G-enabled use cases. Although 3GPP provides 5G infrastructure security specifications, there is a need for additional standard bodies at the intersection of 5G and technologies such as blockchain, IoT and autonomy. Public-private partnerships can be leveraged to develop de facto standards and promote best practices for 5G security implementation and 5G secure supply chains that other countries may come to adopt.

These efforts will benefit from government funding focused on realising: (i) standards-compliant network stacks for 5G and beyond that are open-source and secure by design to encourage the decoupling of the software and hardware ecosystems of 5G; these, in turn, will mitigate the threat posed by supply-chain attacks and promote 5G vendor diversification and market competition; (ii) innovation support for start-up companies; (iii) international collaboration and partnerships that create joint academic and research programmes centred on 5G; (iv) participation in standards bodies responsible for 5G and related technologies; and (v) exchange programs among leading research universities in NATO nations and its strategic partners such as South-Korea, Japan and Australia.

6. CONCLUSION

There is widespread awareness by governments and industry of the great potential for economic development that comes with 5G and of the new security vulnerabilities that come with it. More than in previous generations of mobile systems, there is also open discussion of the geopolitical factors in play. Specific concerns about security and privacy in the context of major Chinese 5G vendors have led to widely publicised discussions between US national security officials and their counterparts in allied nations.

The defence and national security apparatuses in many countries are grappling with how they can adopt 5G as part of their own critical communications infrastructure. In doing that, they face questions including military and civilian spectrum-sharing, adoption of open source implementation and securing the supply chain. It is appropriate, therefore, that NATO plays a role in

5G innovation and security by design, in sharing of 5G threat intelligence and in the certification of 5G security solutions.

We argue that increased cooperation among NATO nations and its strategic partners is vital to effectively face the new challenges brought by 5G. A role for NATO in serving as a forum for collaboration in 5G security across the Atlantic and expanding that collaboration through its diplomatic dialogues has also been recently advocated by others (Chivot and Jorge-Ricart, 2020). The development of a common 5G security strategy across the Atlantic would be the critical first step towards implementing the recommendations in this chapter. A common strategy, with buy-in from key stakeholders in government and industry, could lead to the creation of joint research programmes, harmonised spectrum allocation, a united front on the development of standards and incentives to accelerate intellectual property and innovation. 6G is already starting to be discussed: to regain the leadership in 5G and its successors, NATO nations will need to incentivise close collaboration between academic researchers, relevant NATO Centres of Excellence, NATO entities, private industry and regulators in NATO nations working together towards a common goal. Modest funding by the European Commission exists for international research collaboration in 5G, but this would need to be increased significantly with coordinated participation from funding agencies across the Atlantic to achieve the level of effect that we advocate in this article.

Such a joint strategy could also lead to more effective and coordinated participation by NATO nations and non-NATO EU member states in the standardisation of 5G and subsequent generations. It could also affect the adoption and success of new technologies, like open source initiatives for the 5G radio access network being championed by the O-RAN Alliance (2020) that can have a profound impact on the supply chain of these future networks.

7. REFERENCES

Afolabi, I., Taleb, T., Samdanis, K., Ksentini, A., & Flinck, H. (2018) Network slicing and softwarization: A survey on principles, enabling technologies, and solutions. *IEEE Communication Surveys and Tutorials.* 20 (3), 2429–2453.

Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019) Security for 5G and beyond. *IEEE Communication Surveys and Tutorials.* 21 (4), 3682–3722.

Chivot, E., & Jorge-Ricart, R. (2020) *The EU's approach to 5G and the reshaping of transatlantic relations.* European Leadership Network. Available from: https://www.europeanleadershipnetwork.org/commentary/the-eus-approach-to-5g-and-the-reshaping-of-transatlantic-relations/ [Accessed 19th October 2020].

Corvus Insurance. (2020) Security Report. Available from: https://info.corvusinsurance.com/hubfs/Security%20Report%202.2%20-%20Health%20Care%20.pdf [Accessed 16th November 2020].

Cremers, C., & Dehnel-Wild, M. (2019) Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion. In Network and Distributed Systems Security Symposium (NDSS).

CTIA Certification. (2020) *IoT cybersecurity certification program management document* Available from: https://api.ctia.org/wp-content/uploads/2020/ 05/ CTIA-IoT-Cybersecurity-Program-Management-Document-Ver-1.2.pdf [Accessed: 4th August 2020].

Cybersecurity and Infrastructure Security Agency (CISA). (2019) *Overview of risks introduced by 5G adoption in the United States* (tech. rep.) Available from: https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf [Accessed 1st October 2020].

Department of Defense (DoD). (2020) *Department of Defense 5G strategy* (tech. rep.). Available from: https://www.cto.mil/wp-content/uploads/2020/05/ DoD_5G_Strategy_May_2020.pdf [Accessed 1st October 2020].

ENISA. (2018) *Information Sharing and Analysis Centers (ISACs): Cooperative models* Available from: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models [Accessed 3rd August 2020].

European Union. (2019) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/213 (Cybersecurity Act). Available from: https://eur-lex.europa.eu/legal-content/EN/ TXT/PDF/?uri=CELEX:32019R0881&from=EN [Accessed 1st October 2020].

Frost & Sullivan. (2020) 5G and Cybersecurity Implications for Enterprises. Technical Report.

GSMA. (2020) *5G spectrum: GSMA public policy position*. Available from: https://www.gsma.com/spectrum/wp-content/uploads/2020/03/5G-Spectrum- Positions.pdf [Accessed 1st October 2020].

Hussain, S. R. et al. (2019) 5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol. In ACM SIGSAC Conference on Computer and Communications Security (CCS), 669-684.

IBM. (2018) *Blockchain for multinational information sharing.* Available from: https://www.ibm.com/blogs/blockchain/2018/06/blockchain-for-multinational-information-sharing/ [Accessed 11th September 2020].

Iplytics. (2019) *Who is leading the 5G patent race?* Available from: https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race 2019.pdf [Accessed 30th July 2020].

ITU-T. (2019) X.1215: *Use cases for structured threat information expression* Available from: file:///Users/connect_user/Downloads/T-REC-X.1215-201901-I!!PDF-E.pdf [Accessed 21st September 2020].

Jover, R., & Marojevic, V. (2019) Security and protocol exploit analysis of the 5G specifications. IEEE Access 7, 24956-24963.

Kaska, K., Beckvard, H., & Minárik, T. (2019) *Huawei, 5G and China as a security threat* Available from: https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/ [Accessed 16th November 2020].

Kim, H., Kwon, H., & Kim, K. K. (2019) Modified cyber kill chain model for multimedia service environments. *Multimedia Tools and Applications*. 78 (3), 3153–3170.

Liu, M., Mao, Y., Leng, S., & Mao, S. (2018) Full-duplex aided user virtualization for mobile edge computing in 5G networks. *IEEE Access*. 6, 2996–3007.

Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017) A survey on mobile edge computing: The communication perspective. *IEEE Communication Surveys and Tutorials*. 19 (4), 2322–2358.

MITRE. (2020) ATT&CK *Matrix for Enterprise.* Available from: https:// attack.mitre.org/ [Accessed 4th August 2020].

NIS Cooperation Group. (2019) EU coordinated risk assessment of the cybersecurity of 5G networks. Technical Report.

NIS Cooperation Group. (2020) *Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures*. Available from: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating- measures [Accessed 3rd August 2020].

Office of the Inspector General of the Intelligence Community. (2019) *Unclassified joint report on the implementation of the Cybersecurity Information Sharing Act of 2015.* Available from: https://www.oversight.gov/sites/default/files/oig-reports/Unclassified%2020191219_AUD-2019-005-U_Joint%20Report.pdf [Accessed 21st September 2020].

O-RAN Alliance. (2020) Operator Defined Next Generation RAN *Architecture and Interfaces*. Available from: https://www.o-ran.org/ [Accessed 1st October 2020].

Riaz, H., & Tahir, M. A. (2018) Analysis of VMware virtual machine in forensics and anti-forensics paradigm, In International Symposium on Digital Forensic and Security (ISDFS).

Sexton, C., Kaminski, N., Marquez-Barja, J., Marchetti, N., & DaSilva, L. (2017) 5G: Adaptable Networks Enabled by Versatile Radio Access Technologies. *IEEE Communications Surveys and Tutorials*. 19 (2), 688-720.

Sharevski, F. (2018. Towards 5G cellular network forensics. EURASIP Journal on Information Security. 8.

Tank, D., Aggarwal, A., & Chaubey, N. (2019) Virtualization vulnerabilities, security issues, and solutions: A critical study and comparison. International Journal of Information Technology.

US Congress. (2015) Cybersecurity Information Sharing Act of 2015. Available from: https://www.congress.gov/bill/114th-congress/senate-bill/754 [Accessed 1st October 2020].

White House. (2020) National strategy to secure 5G of the United States of America. Technical Report.

The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO

Jacopo Bellasio
Senior Analyst
Defence, Security and Infrastructure
RAND Europe

Erik Silfversten
Co-Director
Centre for Futures and Foresight Studies
RAND Europe

Abstract: Recent years have seen significant advances in a wide array of new and emerging technologies with disruptive potential, several of which have an inherent cyber dimension. These include, inter alia, artificial intelligence and machine learning, autonomous devices and systems, telecommunications and computing technologies, satellites and space assets, human-machine interfaces and quantum computing. This paper provides an overview of some of the key technology trends for the coming decade and their potential implications for the future cyber threat landscape and NATO. The paper provides an overview of challenges that could emerge from individual technologies, from complex interactions between them, as well as with broader socio-economic trends. It also discusses how technological change and development may occur at such a pace, and have such wide-ranging impact, that NATO and its member states could struggle to achieve its mission and objectives. It concludes by putting forward a set of considerations for preparing for, responding to, and mitigating these challenges.

Keywords: *Cyber security, future threats, emerging threats, disruptive technologies*

1. INTRODUCTION

What cyber threats could emerge over the next decade from new and emerging technologies? How could NATO prepare for and manage them? Recent decades have seen a revolution in Information and Communication Technologies (ICTs) and related technology areas. The development, proliferation, widespread use and embedding of ICTs in contemporary societies have resulted in unprecedented change affecting all aspects of human activity, including military and foreign affairs.

In defence, this has been evident in cyber security and network defence, but has also contributed to the growth of hybrid threats[1] and wider threats in the information environment. In this context, NATO and its member states are facing growing challenges from state and non-state actors in cyberspace, with threats to the Alliance's integrity and military operations and to the day-to-day functioning of its institutions (NATO, 2020a).

In parallel with these developments, we have seen significant advances in a wide array of new and emerging technologies that could have disruptive implications to the nature, scope and potential impact of cyber threats to NATO. The pace of technological change is expected to continue in the next decade and may have profound effects on defence and security matters (Kepe et al., 2018). The rapid pace of change, the complexity and the uncertainty of these developments require an understanding of their implications to ensure NATO's ability to ensure resilience and manoeuvrability in the cyber domain.

This paper discusses a selection of new and emerging technologies with potentially disruptive effects, particularly concerning cyber threats that may stem from their maturation and use over the next decade. It concludes by presenting cross-cutting implications to the future cyber threat landscape before offering thoughts for possible actions to be implemented by NATO and its member states. Given the breadth of technologies considered, this paper is meant to provide an introductory overview of new and emerging technologies, particularly for a non-specialist decision-maker audience. The chapter focuses on implications for the future cyber threat landscape, so it does not discuss effects on defence capabilities or on ways in which threats could be mitigated.

2. NEW AND EMERGING TECHNOLOGIES OF RELEVANCE FOR THE FUTURE CYBER THREAT LANDSCAPE

Deep uncertainty characterises the future geostrategic context and how the technology and cyber threat landscapes will develop. The latter issues

[1] Threats comprising of a mix of coercive and subversive activities and tactics, leveraging both conventional and non-conventional methods below the threshold of war to achieve a range of diplomatic, military, economic, and political objectives.

put cyber security and defence professionals, as well as the institutions and communities they protect, at a structural disadvantage, favouring attackers over defenders. Gaining an improved awareness of how the cyber threat landscape may evolve in the next decade could help decision-makers anticipate threats and coordinate timely and effective responses to future challenges. This paper aims to contribute to such efforts by looking at how technological developments may affect the cyber threat landscape over the next decade.

To identify the most relevant new and emerging technologies that could affect that landscape, the authors reviewed the science and technology (S&T) horizon-scanning database of RAND Europe's Centre for Futures and Foresight Studies (CFFS). The CFFS continuously and systematically captures publicly available reports of the latest S&T developments across a wide range of disciplines and fields. At present, the database comprises over 3,000 technology items relevant to security and defence identified from sources in English, Russian and Mandarin. The horizon-scanning approach underpinning the database combines bibliometric and scientometric approaches with expert engagement activities and assessments.

Overall, the following new and emerging technology clusters were deemed most relevant from a NATO perspective in terms of expected effect on the cyber threat landscape: artificial intelligence and machine learning; autonomous devices and systems; telecommunications and computing technologies; satellites and space assets; human-machine interfaces; and quantum computing. While other technology clusters and clustering approaches could have been selected, the authors selected these technologies based on a combined assessment of their likelihood to achieve significant advances over the next decade, and of their potential impact on the cyber threat landscape should these advances materialise.

A. Artificial Intelligence and Machine Learning

Multiple definitions of artificial intelligence (AI) exist. This paper takes AI to refer to a capability within computer systems to perform tasks that would otherwise require human intelligence to be conducted. AI systems can be classified according to a variety of parameters, including their levels of autonomy and sophistication (McCarthy, 2007; Joshi, 2019; Wong et al., 2020). AI systems can also be underpinned by machine learning (ML), which is the science of creating intelligent computer programs that can automatically improve their performance through experience (i.e., 'learning').

AI and ML have already enabled the development of a wide range of applications to make systems more efficient and scalable and for the delivery of tasks that can exceed the capabilities of humans. From an adversarial perspective, AI/ML could be leveraged for nefarious purposes to automate cyber attacks. While the use of AI/ML for such purposes has not yet been observed in the wild, companies have already launched 'red teaming as service' platforms offering automated attack services which combine a confidence engine with

target temptation analysis to detect system and network vulnerabilities, highlighting assets with the highest perceived adversarial value (Randori, 2019). Data collection and AI/ML advances could also be used in the future to analyse large, complex data sets collected and analysed in real-time from the operational environment with predictive aims or to support decision making at the strategic, operational and tactical levels. In this context, holding AI dominance or a competitive advantage could result in AI/ML acting as a critical force multiplier for military capabilities (Waltzman et al., 2020; Williams, 2020).

Concerns have, however, been raised over the current limitations of security evaluations for AI systems and methods, stemming from the lack of a common language to discuss the vulnerability of such systems and more broadly from oversight in terms of assessing the security of AI incorporated in broader applications and systems (Hartmann & Steup, 2020). The proliferation of AI systems has also given rise to the development of so-called adversarial AI, a set of tactics designed to cause ML models to behave in ways desired by adversaries. Adversarial AI has been highlighted as a significant area of concern, particularly for those AI systems designed with humans 'out-of-the-loop' and in those systems where erratic AI behaviour and readings could degrade human situational awareness (Danks, 2020). Defence applications leveraging AI to support decision making on the battlefield or in the context of broader missions and operations could be subject to similar attacks, with an impact on NATO.

AI/ML have also been used to generate so-called 'deep fakes', synthetic media where individuals' likeness are simulated or replaced with those of others (Cauduro, 2018). Deep fakes may be used by hostile actors for propaganda, offensive or covert purposes. For example, highly realistic deep fakes could be used to support influence operations and broader hybrid tactics. Similarly, AI-powered bots on social media could become increasingly difficult to distinguish from human users, making their harnessing for propaganda and influence operations purposes more effective. Recent advances in AI include software that can deploy deep fakes live, for instance in the context of online video conferencing, or algorithms that can alter audio-visual media to change speakers' speech by editing, adding or deleting content (Cole, 2019; Myers, 2019). Such capabilities could be used to influence the trajectory of public discourse, undermine social cohesion and polarise political debates within and between NATO member countries, or to drive a wedge between NATO and local populations in an area of NATO operations (NATO, 2020b).

B. Autonomous Devices and Systems

Autonomous devices and systems are platforms and devices that can achieve their goals independently and require little or external control and supervision. They combine intelligent software which, thanks to AI-enabled autonomy, conducts or assists with decision-making via hardware devices which interact with the system's surroundings and the physical world to collect data and undertake tasks (Scharre, 2018; Vallor and Bekey, 2017).

Autonomous systems can vary in size, hardware and level of autonomy. The level of autonomy is typically classified according to the expected 'meaningful human control', which is a metric reflecting the extent to which humans are required to intervene in a system's interactions with the real world (Scharre, 2018; Fong, 2019; Leikas et al., 2019).

A wide array of autonomous systems with direct relevance to security and defence have been developed in recent years, including autonomous unmanned vehicles, unmanned weapons systems and smart medical devices. Further advances in this field are expected to stem from developments in swarming technologies[2] and of more sophisticated autonomous systems, including for autonomous weapons. These advances are expected to reduce reliance on humans for decision-making or operational control, thus opening vulnerabilities for the possible disruption and manipulation of autonomous systems.

From a cyber threat perspective, the proliferation of autonomous systems and devices is expected to increase the attack surface available to adversaries and malicious actors (Bogan & Feeney, 2020). For example, autonomous weapons systems that include a tether, enabling the remote control of a system from a supplying country wishing to ensure compliance of the use of its systems with international humanitarian law, could result in the embedding of back doors and kill switches limiting the value of autonomous system assets and potentially making them vulnerable to disruption or manipulation by other third parties (Kajander et al., 2020). Similarly, the use of autonomous vehicles for logistics could be targeted by adversaries leveraging cyber vulnerabilities or adversarial AI to disrupt the logistics and supply chains of a military operation (Danks, 2020; Bogan & Feeney, 2020).

C. Computing, Data Storage, Sensors and Telecommunications Technologies

Computing power and data storage technologies are fundamental enablers of ICT systems. Along with sensors, these technologies allow the capture, manipulation and storage of data. Advances in these fields have led to the development of sophisticated capabilities able to record, store and manipulate expanding datasets at increasing speed. Over the next few years, advances for computing technologies are expected to lead to increasing miniaturisation and greater power, enabling a variety of new solutions such as miniaturised supercomputers, semiconductors and microprocessors like 'smart dust' (Shaikh et al., 2016; Beijing Innovation Centre for Future Chips, 2018). With regard to data storage, in addition to the development of high-density low-energy consumption data storage solutions, it is expected that the future will see a continuation of the growing use and reliance of cloud storage technologies, enabling ubiquitous, on-demand access to data through remote servers (Hess et al., 2019).

These trends and their effects are expected to be further reinforced by advances

[2] The development of advanced collective behaviour mechanisms that enable two or more autonomous systems to operate collectively.

in the fields of sensors. Sensors are used on IT-enabled systems to acquire data to contribute to the performing of different tasks, including decision-making and the tracking and monitoring of a variety of different phenomena. Advances in sensors are expected to result in improved performance and accuracy, further miniaturisation[3] and improved ability to record or generate new types of data. From a defence standpoint, modern platforms and systems have already witnessed the embedding of an increasing number and type of networked sensors which monitor and support their performance. In the coming decade, sensors could also see a growing integration at the level of individual soldiers or systems to improve communications, situational awareness and enable more robust decision-making at different levels through data fusion and analysis (Kepe et al., 2018).

These trends are expected to be further reinforced thanks to advances in telecommunications infrastructure. Telecommunications technologies comprise all the physical and digital infrastructure that enables information to flow across the internet and between devices and systems. The global telecommunication infrastructure is expected to continue evolving rapidly and already encompasses a wide range of technologies including Wi-Fi, optical fibre, light-fidelity and fifth-generation mobile networks (5G) (Deloitte, 2017; ENISA, 2019). Advances in telecommunications technologies in the next years are expected to increase bandwidth, decrease latency and increase spectral efficiency, leading to greater connectivity and a more digitalised world.

The coming decade is likely to see a continuation of the shift from offline to online, with more devices, systems and services becoming digital and connected, including in critical infrastructure sectors (Bogan & Feeney, 2020). This will extend to military platforms and activities, providing for a greater impact of cyber threats beyond the cyber domain to traditional military domains of operations and the day-to-day functioning of military institutions (Kepe et al., 2018). Sensors, computing, data storage and telecommunications technology are therefore expected to play a key enabling role for trends and challenges discussed in Section Three of this chapter.

D. Satellites and Space Assets

Satellites and space assets comprise all those technologies that facilitate access to and maintain superiority within orbital and sub-orbital environments in support of ground-based operations. Under this umbrella fall a wide variety of systems and instruments including expendable and reusable launch vehicles, High Altitude Pseudo Satellites (HAPS) and novel satellites. Space assets and technologies also comprise space-based systems supporting ground operations (e.g., for sensing, navigation, or communication) and counterspace and anti-satellite systems (e.g. anti-satellite missiles and jamming technologies) (Black, 2018; Kepe et al., 2018; ESA, 2018; Unal, 2019).

[3] I.e. a trend to manufacture ever smaller mechanical, optical and electronic products and devices.

Future advances in this field are expected to result in progressively reduced technological and financial barriers, encouraging greater activities in space. For instance, commercial space launches and the broader commercial use of space are expected to continue growing after having witnessed significant growth in the last decade (Space Policy Online, 2020). This, in turn, could result in an increasingly congested operating environment where it may be difficult to monitor and distinguish threats from non-threats. Broader advances in space technologies are also expected to enable them to perform a wider array of functions and further expand the contribution and critical enabling that space technologies can offer to ground operations. Low-orbiting small satellites may improve situational awareness, for example by transmitting high-resolution, real-time video directly into the cockpit of military aircraft (Space News, 2019). HAPS could be used to better monitor crises and adversarial activities, as well as to develop more accurate and reliable navigation capabilities (ESA, 2020).

From a NATO perspective, space-based assets already provide critical enabling functions to most military engagements and operations occurring across the land, air, cyber and maritime domains. In turn, satellites and most space assets are characterised by a complex supply-chain and by a significant degree of dependence on cyber-based enabling capabilities. Advances in space technologies and their further embedding in NATO's daily operations could result in cyber threats and vulnerabilities associated with these technologies disproportionately affecting NATO missions and operations (Unal, 2019). As the space domain becomes accessible to actors other than a small cohort of technologically advanced states, the volume and significance of cyber threats against space systems are expected to increase. In this context, threat actors could leverage jamming, spoofing and hacking attacks on communications networks, hijacking of satellites' control systems and mission packages or conduct, as well as cyber attacks on-ground infrastructure and their associated cyber assets (e.g., data centres) (Unal, 2019; Livingstone & Lewis, 2016).

E. Human-Machine Interfaces

The coming decade is likely to see not only an increase in technology use and reliance but also a growing integration of human and machine. As technological systems continue to grow in scale and complexity, humans are likely to expand their role as users of technology to become purveyors, operators and exploiters of these systems (Yanakiev, 2020). Brain-computer interfaces (BCI) and human-machine interfaces (HMI) enable the connection of the human nervous system to electromechanical systems, leveraging advances in neural engineering, nanotechnology and computational neurosciences (Ienca & Haselager, 2016). BCI and HMI are still emerging research areas, but promising technologies and applications have already been illustrated by industry, including brain-controlled computer systems, robotic limbs, neuro-prostheses, brain-stimulators, cognitive orthotics and hearing and visual implants (Chai et al., 2017).

BCI, HMI and wider human-machine teaming have also attracted significant interest from the defence sector with several areas under investigation, including brain-controlled weapons systems, drone swarms and training and exercise applications (Chai et al., 2017; Tucker 2018). HMI has also been particularly explored in relation to manned and unmanned aircraft where it is perceived to be able to facilitate improved information handling and enhance the human operator's effectiveness (Lim et al., 2018). For example, the US Defense Advanced Research Projects Agency (DARPA) is developing an HMI system aimed at reducing pilot workload, augmenting mission performance and improving aircraft safety. It is known as the Aircrew Labour In-Cockpit Automation System (ALIAS). The coming decade is likely to see further integration of humans and machines across society, including in defence, and may prove to offer hitherto unattainable performance in data processing, analysis and decision-making support.

The implications for NATO may, therefore, be wide-ranging and considerable. The shift from humans simply being users of technology towards being part of a complex and connected technological system will both bring opportunities for capability improvement and new vulnerabilities and risks. The future adoption of HMI within NATO and its member countries will require significant efforts in developing appropriate technology and processes across the doctrine, organisation, training, materiel, leadership, personnel, facilities and interoperability (DOTMLPF-I)[4] spectrum, including the relevant knowledge, skills and abilities needed for human-machine integration. The closer integration of humans and technological systems may also lead to significant cyber vulnerabilities that could be exploited by adversaries by, for example, compromising the integrity of information from an HMI to the human operator, such as a pilot, thereby increasing the risk of operator error or failure. Through HMI, humans will comprise a significant part of the system and their behaviour may thus affect the level of system security that can be achieved. The human aspect of cyber security is an emerging area of knowledge and research and substantial efforts are likely to be required to achieve cyber-secure HMI in the future.

F. Quantum Computing

Quantum technologies can be defined as technologies that seek to exploit the properties of quantum science to achieve functions or levels of performance that may otherwise be unattainable or explainable. The properties of quantum science, where subatomic particles (qubits) can exist in two states simultaneously, enable a wide range of novel technologies and applications that go beyond current capabilities. Prominent emerging quantum technology areas include quantum computing, which can enable parallel, faster and less energy-consuming data processing (Innovate UK, 2019), quantum communications, quantum cryptography (Pirandola et al., 2019), quantum sensors (UK Government Office for Science, 2016) and quantum clocks (European Commission Joint Research Centre, 2016).

[4] DOTMLPF-I is a way of describing the essential elements of military capability development (NATO, 2016).

Quantum advances may result in transformational and fundamental shifts in several S&T areas, making their time of realisation and effect inherently difficult to predict. Fully realised quantum computers may be able to overcome the performance limitations of current computing approaches by enabling the parallel processing of data with hugely improvedl speed, precision and detail, potentially revolutionising the future information environment. Within the cyber domain, advances in quantum cryptography could compromise current encryption approaches, posing fundamental challenges to the integrity and security of all NATO data and communications. Further advances in quantum sensing and timing may also create new types of information or insights, contributing to advances in situational awareness and shedding light on previously opaque complexity that can be exploited by NATO and adversaries alike. As with many emerging technologies, quantum technologies may have a 'first mover' advantage that offers potentially significant advantages to the first adopter.

3. DISCUSSION—CROSS-CUTTING THREATS AND IMPLICATIONS

Technological developments and trends of the types discussed in this paper are expected to have profound effects on all levels of society in the coming decade, including on NATO, its member states and its missions and operations. The research cited in this paper also suggests that these technologies will have a significant effect on the cyber threat landscape and, perhaps more concerningly, that the pace and impact of technological change may be so profound that the ability of NATO and its member states to cope with them is surpassed. If the Alliance is unable to keep pace with technology, it may find itself at a disadvantage compared to its adversaries or subject to technological vulnerabilities that could be exploited by adversaries.

In this context, successfully leveraging new and emerging technologies in a timely manner will be key to ensuring NATO's ability to maintain a technological edge in critical areas, including in cyberspace. While we have previously discussed cyber threats that may stem from developments in specific technology areas, these technologies will not operate in silos in the future but rather build on and interact with one another in ways that will result in additional, broader trends and challenges. From a cyber threat perspective, an array of cross-cutting trends and implications should be highlighted and considered by NATO in the coming decade.

A. Complex Synergies and Effects

The most significant impact on the cyber threat landscape will not stem from any individual technology but rather from the complex interaction and combination of different new and existing technologies and broader interplay with the socio-technological environment. The degree of penetration and pervasiveness that new and emerging technologies will achieve over the next decade is expected to span across defence, security, critical infrastructure

and the overall day-to-day functioning of societies. This is likely to significantly increase the volume and impact of threats, vulnerabilities and disruptions associated with digital technologies and societal systems that depend on ICTs. Beyond the volume of potential threats, the coming decade is also likely to further compound the competitive advantage for attackers as malicious actors and adversaries will be less constrained in leveraging emerging technology for offensive purposes due, for example, to their reduced regulation, lower ethical or moral standards, or fewer requirements for testing and validation. This is particularly prominent in the cyber domain, where adversary activities are perceived as low-risk due to attribution challenges, difficulties in cross-border cooperation, differing national laws, lack of adequate legislation and diverging normative views of responsible behaviour in cyberspace (Rid & Buchanan, 2015).

The wide penetration and pervasiveness of emerging technologies may also result in cascading effects which could be difficult to predict or mitigate in increasingly complex and non-linear systems. The exploitation of system vulnerabilities or system failures may result in much broader impacts due to previously unforeseen linkages and embedded co-dependencies, potentially even spanning geographical areas and national boundaries. Continuous technology evolution and varying rates of technology development and adoption will also present significant challenges for NATO in monitoring and understanding the interaction of different technologies, particularly in increasingly complex supply chains. Advances in fields such as telecommunications and computing technologies and sensors are expected to achieve maturity over a shorter time frame, partly due to lower barriers to implementation. Conversely, other potentially disruptive technologies such as quantum computing and more advanced forms of AI and autonomous systems are characterised by greater uncertainty as regards their epoch, making it difficult to anticipate and articulate their expected impact over the next decade (Kepe et al., 2018; Bellasio et al., 2020). The complexity of technology adoption and the challenges associated with mapping and monitoring the threats and vulnerabilities associated with them could, therefore, significantly undermine NATO's ability to protect critical digital and physical infrastructure and retain information superiority.

Much of the innovation and envisioned advances are expected to occur in the private sector through non-defence companies that may be reluctant to support military programmes. For example, cultural and interest divides between the US Department of Defence and the US technology sector have resulted in strained collaborations and the cancellation of several R&D programmes including in AI and facial recognition programmes (Zegart & Childs, 2018). In contrast, China's military-civil fusion policy seeks to foster innovation in several emerging technology areas through an array of policies and other government-controlled mechanisms (US-China Economic and Security Review Commission, 2019). Much innovation in emerging technologies is also taking place in non-NATO countries: China, for example, is emerging as a leader in quantum science (Kania & Costello,

2018) and Japan, South Korea and Taiwan are leaders in areas such as sensors and controls for autonomous vehicles and flexible electronics (Alliance for Manufacturing Foresight, 2019).

This adds further layers of complexity to the challenge and could put NATO and its member states at a disadvantage, limiting access to technological innovation and putting the Alliance and its institutions in a reactive position. This is particularly concerning as an increasing number of services and key enabling technologies are developed and supplied by a limited number of companies and service providers outside NATO's influence or control, which could jeopardise or undermine the security of NATO's supply chains. This could, for example, result in embedded vulnerabilities or unknown systemic weakness that could be used to gain access to critical mission systems or cause significant cascading or systemic disruptions.

B. Hybrid or Sub-Threshold Activities

Several new and emerging technologies have and will continue to facilitate the adoption of hybrid tactics and the undertaking of activities below the threshold of war with increased difficulty in attributing and understanding adversaries' activities and their impact (Thiele, 2020). Advances expected in AI, telecommunications and computing technologies and autonomous systems could facilitate improved ways of delivering known methods, such as deep fakes or the creation of mis- or disinformation, or the creation of entirely novel attacks and approaches. This could include the proliferation of real-time video deep fakes at scale (Seymour, 2018) or advanced voice manipulation (Vincent, 2020) which adversaries could use to manipulate messages from policymakers and military commanders.

Such activities could include, for example, election meddling, influence operations and economic coercion. Such advances present serious risks to the information environment and could undermine NATO, its member states and their institutions by reducing the social cohesion and resilience critical to maintaining socio-economic stability and prosperity. A significant growth in sub-threshold and hybrid activities in the next decade may undermine the integrity and verifiability of data and information. This would make it increasingly difficult to understand where information comes from, where it is going, how and why it was created and who created it, such as, for example, the emergence of competing 'facts' without clear origin that cannot be easily verified or challenged. This could emphasise current trends of misinformation and associated issues, but it could also lead to more consequential systemic effects where the general population loses faith in technology, data or government institutions. These developments may threaten the very foundations of society and will likely require increasingly agile and creative responses from NATO and its member states for their successful mitigation.

C. Exacerbation of Current Trends and Grey Swan Scenarios

The technologies highlighted in this paper may contribute to the exacerbation of current trends in the cyber threat landscape and herald so-called grey swan scenarios.[5] The increasing availability of powerful, easy-to-use and inexpensive technologies is likely to further stimulate the conduct of malicious activities by a wide array of state and non-state actors. The democratisation and 'servitisation'[6] of technology have enabled consumer access to a wide range of technologies that were previously accessible only by governments. This includes enabling technologies like additive manufacturing and large-scale distributed computing, to more niche technological services such as on-demand development of bespoke software-defined radio applications that could be used for disrupting the electromagnetic environment. While most of these activities are likely to entail low-tech tactics, this trend could result in an even greater volume of malicious activities than currently witnessed.

The development of new, complex technological solutions and capabilities may also enable state-sponsored actors to conduct advanced, covert or persistent attacks and activities which could undermine or jeopardise NATO's missions and day-to-day operations by, for example, exploiting unknown vulnerabilities in the NATO supply chain to gain access to sensitive information. Sophisticated and persistent attacks are likely to be less frequent, making these threats more challenging for NATO to identify, detect, prepare for and manage due to limited exposure to and knowledge of the tactics, techniques and procedures (TTP) employed. The proliferation of connected and embedded systems, particularly through a drive towards the Internet of Things (IoT) and the digitalisation of legacy infrastructure may also increase NATO's attack surface and the likelihood of vulnerabilities that could be exploited by malicious actors.

Technological advances are also expected to contribute to an increased ability to record, store, process and analyse data, which will be further compounded by greater connectivity coverage and speeds. The proliferation of new and existing sensors across a growing number of systems and devices will improve data collection capabilities and contribute to the creation and collection of new data types. In the coming decade, these could lead to a near-ubiquitous ability to access and manipulate data, for instance through cloud storage and miniaturised processors. This would provide greater opportunities for the conduct of malicious activities, including through hitherto unseen TTPs, facilitating the exfiltration of sensitive data and making it increasingly difficult to operate without being monitored (Bogan & Feeney, 2020). Increased connectivity, through both an increasing number of connected devices and the adoption of new technologies such as 5G, is

[5] A grey swan scenario refers to an event that could have significant cascading impact that is seen as unlikely, but not impossible.

[6] A trend whereby vendors not only sell products and devices but also offer services. For example, this can result in vendors of certain technologies providing access to enabling or maintenance services for their products, leading to increasingly complex business models, supply chains, liability and ownership arrangements.

also expected to result in an increased volume and speed of activities being conducted, including by adversaries. The proliferation of data may further challenge the ability to identify, detect and attribute malicious activities in Alliance ICT systems and present novel challenges such as difficulties in maintaining privacy and anonymity in datasets. For example, an increasingly rich data environment may enable adversaries to better hide information using steganography techniques to bypass security controls or to exfiltrate sensitive data, also making it more difficult to understand how attacks were perpetrated and who may have been behind them (Cabaj et al., 2018).

With respect to data analysis capabilities, advances in computing power accompanied by developments in AI/ML are expected to contribute to a growing ability to process and analyse data, allowing inferences and results currently beyond the reach of human and current data science capabilities. This trend, perhaps amplified by HMI, could lead to an ability to infer and extrapolate sensitive information from different data types not considered sensitive or threatening when taken in isolation. For example, research has already shown that present-day capabilities allow for the de-anonymisation of incomplete datasets with data on demographic attributes (Rocher et al., 2019).

These advances are expected to contribute to the development of new forms of malicious activities and could hold particularly true in light of the growing potential for the automation and large-scale running of existing malicious activities. Finally, the democratisation of computing power, particularly through the growth of on-demand, scalable and inexpensive cloud data services such as Amazon Web Services and Microsoft Azure, may enable a wider range of actors, including non-state groups, to attain advanced analytical capabilities.

4. SUMMARY AND CONCLUSION

While advances in new and emerging technologies are not expected to be the sole drivers and factors affecting the future cyber threat landscape, their impact should not be underestimated or overlooked. Certainly, the multifaceted and uncertain nature of the future technology landscape, as discussed in section two, and the complex trends and effects expected to stem from it, as presented in section three, will require the adoption of flexible, innovative and forward-looking responses and approaches. No single solution will enable NATO and its member states to respond to the wide array of advances occurring in the technology landscape or to effectively manage new threats in the cyber domain. Bearing this in mind, a number of measures could be considered for adoption by NATO to prepare for future challenges emerging in the cyber threat landscape.

A. Ensuring an Absorptive Capacity for Innovation and Transformation
NATO and its member states need to ensure that the Alliance can prepare for, respond to and exploit advances in the technological and cyber landscapes.

The absorptive capacity – in other words, the ability for NATO to recognise and harness the value of emerging technologies – relies on a complex system with many interacting factors. Previous RAND research has identified several factors that enable innovation and transformation in defence, including organisational culture, input factors such as knowledge, talent and capital, and enabling resources such as infrastructure, networks and connections (Freeman et al., 2015).

NATO should, therefore, consider how best to adapt its organisational culture, civilian and military structures, organisations and agencies to recognise and absorb innovation in the cyber domain in the coming decade. While a range of relevant bodies is already in place including the NATO Science and Technology Organisation, the Emerging Security Challenges Division, the Joint Intelligence and Security Division, the NATO Communications and Information Agency and the Cyber Operations Centre, these considerations may require further adjustments depending on which technology area, or combination thereof, is ultimately pursued. Adjustments could entail placing a specific focus on: (i) whether current procurement processes are fit for purpose; (ii) whether NATO is in a position to contribute to the development and definition of legal and regulatory standards for the use of different technologies; and (iii) the requirements for and availability of adequate testing and assurance mechanisms for the use of emerging technologies in a military context.

B. Enabling the Identification of Emerging Technology Requirements and Cooperation with Industry

Beyond the absorptive capacity for innovation and transformation, NATO must also be in a position to identify emerging technologies of interest, their implications to NATO and what the Alliance's requirements in relation to those technologies may be. As previously noted, being an early adopter or creating a technological edge over adversaries and competitors will be pivotal to enable NATO and its member states to hold a strategic advantage and superiority in the cyber domain. Some of the technologies presented in this paper will also act as enablers, expanding and deepening the impact of other existing and developing technologies.

In this context, NATO should seek to be in a position to gather intelligence continuously and systematically on emerging science and technology developments and their potential implications for NATO through approaches such as strategic foresight analysis, horizon scanning, scenario planning and analytical gaming. This will enable the Alliance to improve its posture and agility with early warning signs of technologies that may be exploited by adversaries in the future. Activities in this regard are ongoing through Allied Command Transformation Strategic Foresight Analysis (e.g., ACT, 2017), the NATO Science and Technology Organisation and NATO education and training institutions such as the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Defence College (e.g., Gilli, 2020). The work of other NATO Centres of Excellence could also facilitate the identification and

monitoring of relevant technologies of interest across different areas.

A fundamental part of ensuring this will be close consultation and cooperation with industry. Many of these emerging technologies will be primarily developed in the private sector and often by companies that traditionally have not worked within the defence sector. NATO must therefore be able to clearly communicate its innovation and transformation needs and explain why it may be worthwhile for non-traditional defence suppliers to support defence needs and engage with the Alliance. It is also essential that NATO encourages and enables its member states to leverage the expertise and knowledge found in the private sector to understand the state-of-the-art in the different emerging technology areas and what opportunities or risks they may bring. This entails enabling and maintaining partnerships that go beyond customer-supplier relationships and should involve structures for innovation where inventors, investors and industry can partner with NATO across a wide range of emerging technology areas to better meet the cyber challenges of the coming decade. In this regard, the NATO Industry Cyber Partnership has already laid the foundation for engagement between NATO and industry in the cyber domain that goes beyond information sharing for improved situational awareness to building trust and access between NATO and the private sector, including for capability development purposes (NICP, 2018). NATO Smart Defence could also act as an example on which to build the blueprint for identifying requirements and cooperatively generating future capabilities, bringing together not just Alliance members, but industry representatives and stakeholders more broadly (NATO, 2017).

C. Strengthening Trust and Interoperability Across the Alliance

The coming decade will be of pivotal importance to NATO as a period characterised by a continuously evolving technology landscape with potentially disruptive effects in the cyber domain and beyond. In an era of uncertainty, constrained resources and political tension, cooperation and trust will be fundamental enablers of an agile, technology-driven and digital NATO. Only through joint efforts will NATO truly be able to harness the potential of the emerging technologies discussed in this chapter and successfully mitigate the risks and threats they may pose in the future. The need for trust therefore extends to both trust in technology and trust in the Alliance and its member states.

Similar to how the effects of emerging technologies should not be treated in isolation, NATO's response to emerging technologies must be one of joint efforts and interoperability. Technical, legal, financial and organisational barriers to the implementation of emerging technologies are more likely to be overcome through joint capability and force development efforts, which will, by extension, also help build trust and facilitate interoperability. Several of the emerging technology areas discussed in this paper would place significant data, infrastructure and interoperability requirements on NATO, which may be particularly difficult to overcome given the current state of data heterogeneity and sometimes incompatible digital infrastructure across the

Alliance. Several emerging technologies would also require interoperability in relation to shared vocabularies of technical terms, norms, standards and organisational practices, as well as human interoperability and joint training and exercising. For example, AI has been highlighted as a potential area of concern where a lack of interoperability and common definitions paired with technological mismatches could erode Alliance cohesion (Dufour, 2018).

Joint efforts are, therefore, likely to help overcome these challenges and barriers to NATO harnessing emerging technologies in the next decade. While the 30-member Alliance may be at a competitive disadvantage compared to single state or non-state adversaries in relation to interoperability barriers, NATO's collective strength may also serve as an enabler for technological superiority. Joint planning, requirement setting, and development may enable individual member states to pursue specialisation in aspects of particular emergent technology areas, thereby allowing other countries to pursue other specialisations and, by extension, increasing the overall capability within the Alliance.

5. REFERENCES

Allied Command Transformation. (2017) Strategic Foresight Analysis 2017. Available from: https://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf [Accessed 20th October 2020].

Alliance for Manufacturing Foresight. (2019) 'Reclaiming America's Leadership in Advanced Manufacturing'. Available from http://mforesight.org/download-reports/ [Accessed 24th September 2020].

Beijing Innovation Centre for Future Chips. (2018) White Paper on AI Chip Technologies. Available from: https://www.080910t.com/downloads/AI%20Chip%202018%20EN.pdf [Accessed 21st August 2020].

Bellasio, J., Silfversten, E., Leverett, E., Quimbre, F., Knack, A. & Favaro, M. (2020) *The future of cybercrime in light of technology developments.* Prepared for the European Commission Structural Reform Support Service (Ref: SRSS/C2018/092).

Black, J. (2018) 'Our reliance on space tech means we should prepare for the worst'. *Defensenews.com*. Available from https://www.defensenews.com/space/2018/03/12/our-reliance-on-space-tech-means-we-should-prepare-for-the-worst/ [Accessed 21st August 2020].

Bogan, J. & Feeney, A. (2020) *Future cities: Trends and implications.* Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875528/Dstl_Future_Cities_Trends____Implications_OFFICIAL.pdf [Accessed 23rd September 2020].

Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward, A. & Zander, S. (2018) The new threats of information hiding: The road ahead. *IT Professional*, 20 (3), 31-39. Available from: https://arxiv.org/ftp/arxiv/papers/1801/1801.00694.pdf [Accessed 20th October 2020].

Cauduro, A. (2018) Live Deep Fakes – you can now change your face to someone else's in real time video applications. *Medium*. Available from: https://medium.com/huia/live-deep-fakes-you-can-now-change-your-face-to-someone-elses-in-real-time-video-applications-a4727e06612f [Accessed

12th August 2020].

Chai, R., Naik, G.R., Ling, S.H. & Nguyen, H.T. (2017) Hybrid brain–computer interface for biomedical cyber-physical system application using wireless embedded EEG systems. *Biomedical engineering online*. 16 (1), 5. [Accessed 20th August 2020] Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5234249/

Cole, S. 2020 *This Open-Source Program Deepfakes You During Zoom Meetings, in Real Time*. Available from: https://www.vice.com/en_us/article/g5xagy/this-open-source-program-deepfakes-you-during-zoom-meetings-in-real-time [Accessed 23rd September 2020].

Danks, D. 2020 *How Adversarial Attacks Could Destabilize Military AI Systems.* Available from: https://spectrum.ieee.org/automaton/artificial-intelligence/embedded-ai/adversarial-attacks-and-ai-systems [Accessed 23rd September 2020].

DARPA. (2020) *Aircrew Labor In-Cockpit Automation System (ALIAS).* Available from https://www.darpa.mil/program/aircrew-labor-in-cockpit-automation-system [Accessed 24th September 2020].

Deloitte. (2017) *Communications infrastructure upgrade: The need for deep fiber.* Available from: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5GReady-the-need-for-deep-fiber-pov.pdf [Accessed 20th August 2020].

Dufour, M. 2018 Will artificial intelligence challenge NATO interoperability? *NDC Policy Brief.* Available from: http://www.ndc.nato.int/news/news.php?icode=1239# [Accessed 23rd September 2020].

ENISA. (2019) *ENISA threat landscape for 5G network.* Available from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks [Accessed 18th August 2020].

European Commission. (2019) *A definition of Artificial Intelligence: main capabilities and scientific disciplines.* Available from: https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines [Accessed 20th August 2020].

European Commission Joint Research Centre. (2016) *Quantum Technologies: Implications for European Policy*. Available from: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC101632/lbna28103enn.pdf [Accessed 20th August 2020].

ESA. (2018) *Could High-Altitude Pseudo-Satellites Transform the Space Industry?* Available from: https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation/Could_High-Altitude_Pseudo-Satellites_Transform_the_Space_Industry [Accessed 20th August 2020].

ESA. 2020 *Services enabled by High Altitude Pseudo Satellites (HAPS) complemented by satellites.* Available from: https://business.esa.int/projects/services-enabled-haps [Accessed 23rd September 2020].

Fong, T. (2018) *Autonomous systems: NASA capability overview.* Available from: https://www.nasa.gov/sites/default/files/atoms/files/nac_tie_aug2018_tfong_tagged.pdf [Accessed 20th August 2020].

Freeman, J., Hellgren, T., Mastroeni, M., Persi Paoli, G., Cox, K. & J. Black. (2015) *Innovation Models: Enabling new defence solutions and enhanced benefits from science and technology.* Available from: https://www.rand.org/pubs/research_reports/RR840.html [Accessed 21st August 2020].

Gilli, A. (2020) *NATO and 5G: what strategic lessons? NDC Policy Brief.* 13(July 2020).

Available from https://www.ndc.nato.int/research/research.php?icode=0 [Accessed 18th August 2020].

GSMA. (2019) *Mobile Telecommunications Security Threat Landscape.* Available from https://www.gsma.com/security/wp-content/uploads/2019/03/GSMA-Security-Threat-Landscape-31.1.19.pdf [Accessed 18th August 2020].

Hartmann, K. & Steup, C. 2020 Hacking the AI – The Next Generation of Hijacked Systems. In: Jančárková, T., Lindström, L., Signoretti, M., Tolga, I. & G. Visky (eds.) *2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade.*

Hess, J., Kiser, A., Bouhafa, E.M. & Williams, S. (2019) The Combat Cloud: Enabling Multidomain Command and Control across the Range of Military Operations. *Wright Flying Papers, Air Command and Staff College.* February 2019. Available from: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/wf_0065_hess_combat_cloud.pdf [Accessed 14th August 2020].

Ienca, M. (2015) Neuroprivacy, neurosecurity and brain-hacking: Emerging issues in neural engineering. *Bioethica Forum*. 8 (2), 51-3. Available from: https://edoc.unibas.ch/39747/ [Accessed 20th August].

Innovate UK. (2019) *Innovate UK: Global Expert Mission Quantum Technologies in the USA.* Available from: https://admin.ktn-uk.co.uk/app/uploads/2020/03/0183_KTN_USA-QuantumTechnologiesReport_v4.pdf [Accessed 21st August 2020].

Joshi, N. 2019) 7 Types of Artificial Intelligence. *Forbes*. 19 June 2019. Available from: https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/#6eb1f3ad233e [Accessed 21st August 2020].

Kajander, A., Kasper, A. & Tsybulenko, E. (2020) Making the Cyber Mercenary – Autonomous Weapons Systems and Common Article 1 of the Geneva Conventions. In: Jančárková, T., Lindström, L., Signoretti, M., Tolga, I. & G. Visky (eds.) *2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade.*

Katano, Y., Muroi, T., Kinoshita, N. & Ishii, N. (2017) Prototype holographic data storage drive with wavefront compensation for playback of 8K video data. *IEEE Transactions on Consumer Electronics.* 63(3). Available from: https://ieeexplore.ieee.org/document/8103372 [Accessed 18th August 2020].

Kepe, M., Black, J., Melling, J., & Plumridge, J. (2018) *Exploring Europe's capability requirements for 2035 and beyond Insights from the 2018 update of the long-term strand of the Capability Development Plan*. Available from: https://www.eda.europa.eu/docs/default-source/brochures/cdp-brochure---exploring-europe-s-capability-requirements-for-2035-and-beyond.pdf [Accessed 12th August 2020].

Kersting, K. (2018) Machine learning and artificial intelligence: two fellow travelers on the quest for intelligent behaviour in machines. *Specialty Grand Challenge 1.* Available from: https://ml-research.github.io/papers/kerstingg2018aiml_frontiers.pdf [Accessed 12th August 2020].

Leikas, J.; Koivisto, R.; & Gotcheva, N. (2019) Ethical Framework for Designing Autonomous Intelligent Systems. *J. Open Innov. Technol. Mark. Complex.* 5 (1), 18. Available from: https://doi.org/10.3390/joitmc5010018 [Accessed 21st August 2020].

Lim, Y., Ramasamy, S., Gardi, A., Kistan, T. & Sabatini, R. (2018) Cognitive human-machine interfaces and interactions for unmanned aircraft. *Journal of Intelligent & Robotic Systems*. 91 (3-4), 755-774.

Livingstone, D. & P. Lewis. (2016) *Space, the Final Frontier for Cybersecurity?* Available from: https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf [Accessed 23 September 2020].

McCarthy, J. (2007) *What Is Artificial Intelligence? Technical report.* Stanford University. Available from: http://jmc.stanford.edu/articles/whatisai/whatisai.pdf [Accessed 12th August 2020].

Myers, A. (2019) *Stanford engineers make editing video as easy as editing text.* Available from: https://news.stanford.edu/2019/06/05/edit-video-editing-text/ [Accessed 23 September 2020].

NATO. (2016) *Joint Analysis Handbook* Available from http://www.jallc.nato.int/products/docs/Joint_Analysis_Handbook_4th_edition.pdf [Accessed 24th September 2020].

NATO. (2018) *Smart Defence*. Available from: https://www.nato.int/cps/en/natohq/topics_84268.htm [Accessed 23 September 2020].

NATO. (2020a) *Cyber defence*. Available from: https://www.nato.int/cps/en/natohq/topics_78170.htm [Accessed 13th August 2020].

NATO. (2020b) *NATO's approach to countering disinformation: a focus on COVID-19*. Available from: https://www.nato.int/cps/en/natohq/177273.htm [Accessed 23 September 2020].

NATO CCD COE. (2020) *Exercises*. Available from: https://ccdcoe.org/exercises/ [Accessed 23 September 2020].

NICP. (2018) *Our objectives and principles*. Available from: https://nicp.nato.int/objectives-and-principles/index.html [Accessed 23 September 2020].

Pirandola, S., Andersen, U. L., Banchi, Berta, L., M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J., Razavi, M., Shaari, J.S., Tomamichel, M., Usenko, V.C., Vallone, G., Villoresi, P., and Wallden, P. (2019). *Advances in Quantum Cryptography. Quantum Physics*. Available from: https://arxiv.org/abs/1906.01645 [Accessed 12th August 2020].

Randori. (2020) *Randori Recon: Shining Light on Your Most Tempting Targets.* Available from: https://www.randori.com/randori-recon-shining-light-on-your-most-tempting-targets/ [Accessed 23 September 2020].

Rid, T & Buchanan, B. (2015) Attributing Cyber Attacks. *Journal of Strategic Studies*. 38 (1-2), 4-37.

Rocher, L., Hendricks, J.M., & Montjoye, Y. M. (2019) Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications.* 10 (3069).

Scharre, P. (2018) *Army of None: Autonomous Weapons and the Future of War*. London, UK: W.W. Norton & Company.

Seymour, M. (2018) *A.I. at SIGGRAPH: Part 2. Pinscreen at Real Time Live.* Fxguide. Available from https://www.fxguide.com/fxfeatured/a-i-at-siggraph-part-2-pinscreen-at-real-time-live/ [Accessed 24th September 2020].

Shaik, M., Shaik, N., & Ullah, W. (2016) The Wireless Sensor Networks: Smart Dust. *International Research Journal of Engineering and Technology.* 3 (6). Available from: https://www.irjet.net/archives/V3/i6/IRJET-V3I6172.pdf [Accessed 20th August 2020].

Shea, J. (2018) Cyberspace as a Domain of Operations: What is NATO's Vision and Strategy? *MCU Journal*. 9 (2), 133-150. Available from: https://doi.

org/10.21140/mcuj.2018090208 [Accessed 10 August 2020].

Space News. (2019) *U.K. deepens space ties with U.S., announces investments in small satellites, responsive launch*. Available from: https://spacenews.com/u-k-deepens-space-ties-with-u-s-announces-investments-in-small-satellites-responsive-launch/ [Accessed 23 September 2020].

Space Policy Online. (2020) *Commercial Space Activities*. Available from: https://spacepolicyonline.com/topics/commercial-space-activities/ [Accessed 23 September 2020].

Thiele, R. (2020) *Artificial Intelligence – A Key Enabler of Hybrid Warfare. Hybrid CoE Working Paper 6*. Available from https://www.hybridcoe.fi/wp-content/uploads/2020/03/WP-6_2020_rgb.pdf [Accessed 24th September 2020].

Tucker, P. (2018) It's now possible to telepathically communicate with a drone swarm. *Defense One*. Available from https://www.defenseone.com/technology/2018/09/its-now-possible-telepathically-communicate-drone-swarm/151068/ [Accessed 21st August 2020].

UK Government Office for Science. (2016) *The Quantum Age: technological opportunities.* Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/gs-16-18-quantum-technologies-report.pdf [Accessed 21st August 2020].

Unal, B. (2019) *Cybersecurity of NATO's Space-based Strategic Assets. Chatham House*. Available from: https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf [Accessed 21st August 2020].

U.S.-China Economic and Security Review Commission. (2019) *2019 Annual Report to Congress*. Available from https://www.uscc.gov/annual-report/2019-annual-report-congress [Accessed 24th September 2020].

Vallor, S., & Bekey, G. A. (2017) Artificial Intelligence and the Ethics of Self-learning Robots. In Lin, P., Abney, K., & Jenkins, R. (eds.) *Robot Ethics 2.0.* Oxford University Press, pp. 338-353.

Vincent, J. (2020) This is what a deepfake voice clone used in a failed fraud attempt sounds like. *The Verge*. Available from https://www.theverge.com/2020/7/27/21339898/deepfake-audio-voice-clone-scam-attempt-nisos [Accessed 24th September 2020].

Waltzman, R., Ablon, L., Curriden, C., Hartnett, G. S., Holliday, M. A., Ma, L., Nichiporuk, B., Scobell, A. & Tarraf, D. C. (2020) *Maintaining the Competitive Advantage in Artificial Intelligence and Machine Learning*. Available from: https://www.rand.org/pubs/research_reports/RRA200-1.html [Accessed 21st August 2020].

Williams, L.C. (2020) *JADC2 Tops Pentagon's Artificial Intelligence Efforts.* FCW, 9 July 2020. Available from: https://fcw.com/articles/2020/07/09/williams-jaic-ai.aspx [Accessed 13th August 2020].

Wong, Y.H., Yurchak, J.M., Button, R.W., Frank, A., Laird, B., Osoba, O.A., Steeb, R., Harris, B.N. & Bae, S.J. (2020) *Deterrence in the Age of Thinking Machines.* Available from: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2797/RAND_RR2797.pdf [Accessed 12th August 2020].

Xiao, L., Jianying, H., Mingjie, Z., Tiangui, D., Hui L. & Yuhong, R. (2019) Optical holographic data storage — The time for new development. *Opto-Electronic Engineering*. 46(3). Available from http://www.oejournal.org/J/OEE/Article/Details/A190315000012 [Accessed 20th August 2020].

Yanakiev, Y. (2020) Introduction to NATO STO Task Group Hfm-259: Human Systems

Smart Cities, Cyber Warfare and Social Disorder

Simona R. Soare
Senior Associate Analyst
European Union Institute for Security Studies (EUISS)

Joe Burton
Marie Curie Fellow, Université libre de Bruxelles (ULB) and Senior Lecturer
New Zealand Institute for Security and Crime Science
University of Waikato

Abstract: Cyber warfare often targets national security apparatus, but local governance vulnerabilities are just as serious and much less studied. In this paper, we examine the potential impact of cyber warfare directed against smart cities and the relationship between cyber attacks and social disorder in urban spaces. The first part of the paper consists of a foresight scenario that serves to identify operational, procedural, governance and capability gaps in responding to and building resilience against fictional, but possible events. In our foresight scenario, Megalopolinn, the capital of a major European NATO ally, comes under a sustained cyber assault from a network of hackers linked to an authoritarian, revisionist state. We map out the multiple surfaces of cyber attack in a smart city grid and how they contribute to a serious breakdown in the city's social, political and technical structures and processes when combined with other hybrid warfare tactics. The second section is a more conventional academic analysis of existing literature on cities as actors in International Relations and the smart city as an emerging unit of analysis in security policy and planning. The third section provides a comprehensive analysis of the rise of smart cities and the vulnerabilities in smart city infrastructure and technologies, including artificial intelligence (AI) and automation, the Internet of Things (IoT), 5G, social media, synthetic media and deepfakes, and the risks posed to governance structures and capabilities that rely on super-connectivity and complex networks. We highlight three vulnerabilities of smart cities – technological, social and governance-related. This section argues that local governance is potentially an easier attack surface than the national level for malign actors who seek mass disruption and that significant changes in local governance structure and practice are needed to close smart city vulnerabilities, including a better understanding of the links between smart city security and national security.

Keywords: *Smart city, cyber warfare, hybrid warfare, local governance, national security, NATO*

1. DARK DAYS IN MEGALOPOLINN

February 2030. The smart city infrastructure of Megalopolinn is under attack. Megalopolinn is Varmatia's largest city, with over 10 million inhabitants. It generates over 30 per cent of Varmatia's GDP and is a major European transport hub and pivotal to NATO logistics, defence planning, military mobility, and reinforcement of Eastern European allies. Varmatia is bordered by Lusia, a hostile foreign power, with which it has a history of confrontation.

At 19:43, on 2 February, massive AI-enabled Distributed Denial of Service (DDoS) attacks, harnessing the city's millions of IoT devices, cripple Megalopolinn's 5G servers and transmission masts. The smart city's master network has been infected by a self-replicating and self-learning worm, which is rapidly propagating through the smart critical infrastructure grid. Within hours, the malware cascades through different sectors of the grid, disabling City Hall servers and cutting GPS services used by the police and emergency services. The coordinated assault shuts down the power and water supply to half the city's population. Citizens do not have access to clean water or electricity, they cannot heat their houses, withdraw money, communicate with loved ones or city authorities.

Megalopolinn is surrounded by navigable water canals, operated by a fully automated water and navigation management system. The worm infects and manipulates the automated industrial control system of the city's canals and dams, leading to the progressive flooding of an area roughly the size of Brussels. The city provides the largest rail transport hub in central Europe and is relied upon by the EU and NATO for military mobility. The flooding occurs just seven days before the DEFENDER 2030 transatlantic military exercise, which depends on the city's infrastructure for the transit of troops and equipment.

Further fuelling popular anger, a video spreads online depicting Megalopolinn's Mayor deriding the desperation of city dwellers. The European Union (EU) East StratCom Task Force (a key EU instrument tasked with countering misinformation campaigns) reports a spike in anti-Varmatian, anti-EU and anti-NATO 'deepfake' videos—synthetic media produced by AI algorithms (Barnes and Barraclough, 2020). National regulation does not allow their rapid removal without due process. In a public address on national television, the City's Mayor, in violation of cyber response protocols, attributes the attack on his smart city to Lusia. National authorities have not been consulted on this attribution, but Lusia is responding aggressively and threatening massive repercussions.

By 3 February, riots, looting, destruction of property and cases of violence are reported throughout the city. Police response is obstructed by the malware, which has disabled smart alarm systems and CCTV cameras and is preventing law enforcement drones from transmitting data necessary for accurate situational awareness. The rioters, armed with Molotov cocktails, baseball

bats and small arms, have placed barricades along all the main roads into the city, and the underground system has ground to halt.

By 5 February, law enforcement is overwhelmed, and rioters are threatening to break into City Hall. The Varmatian government is ready to declare a national emergency. The Varmatian ambassador to NATO hands in an official request for an urgent North Atlantic Council (NAC) meeting to inform allies of potential disruptions to NATO activities and to present allies with intelligence suggesting the Lusian government is orchestrating a sophisticated cyber and hybrid attack against Megalopolinn.

2. THE BRITTLENESS OF SMART CITIES

As the foresight scenario above demonstrates, smart cities are brittle architectures. From technological, social and governance points of view, they have multiple points of failure with cascading, systemic effects. The purpose of the foresight scenario is not to depict the future but to raise awareness of less visible risks and vulnerabilities—in this case, the interdependencies between smart city grids, local governance and social order. The scenario also serves to highlight how smart city security risks might affect broader national and allied security. Our goal in this paper is to analyse the multiple vulnerabilities, risks and threats faced by smart cities and map out much-needed changes in technological, social and governance approaches to help increase local preparedness and enhance resilience in the face of catastrophic cyber and hybrid events.

What are the main vulnerabilities and threats faced by smart cities? How do we conceptualise them in an allied framework? In an attempt to answer these questions, this paper proceeds as follows. First, we define and analyse the role of cities as actors in international relations and particularly of smart cities as an emerging unit of analysis in security policy planning. Then, we analyse the vulnerabilities, risks and threats faced by smart city infrastructure in cyber and hybrid warfare. We argue that the growing body of literature on the security of smart cities is limited to a primarily technological approach. Smart city vulnerabilities are as much technological as they are human, social and governance driven. For a more comprehensive view, a more encompassing definition of smart cities as synergetic physical, virtual and human systems is required. Furthermore, we argue that a particular focus is needed on clarifying and exercising the connections between smart cities and national security.

A. Cities and International Security

Cities were not the traditional focus of International Relations (IR) or Security Studies literature. During the Cold War, states were the main unit of analysis and were central to realist accounts of international relations. The emergence of the 'national security state' drew particular attention, as the dangers of the Cold War, nuclear arms race and fears of revolutions led to the

creation of powerful security and intelligence apparatus (Raskin, 1976). In the mid-to-late 1980s, however, the focus of IR began to change, and a variety of non-state actors, including terrorist groups and international organisations became the focus of analysis. States were not a 'black box' according to these emerging understandings; what happened inside the state was important in shaping international affairs, and a new range of international theories sought to focus on sub-state actors, identity groups and societal dynamics (Buzan, 1991).

Two emerging trends led scholars to include cities in IR analysis. The first was the trend of globalisation, which increased the political, financial and military relevance of cities and their role as command posts and centres of planning (Alderson et al., 2006). The combination of globalisation's effects and the rapid spread of information and communication technologies (ICTs) made the world 'flat' and global changes had localised effects and vice-versa. The second trend related to urbanisation, a process that has been driven by globalisation, the rise in international markets, industry, the emergence of service-driven economies and job opportunities, and the decline of rural living and economies. Since 2016, over half the world's population has lived in cities, and this is set to rise to two-thirds, an estimated 7 billion people, by 2050 (Ritchie & Roser, 2018).

Cities are not always safe places for people to be. Almost a quarter of people in cities globally live in slum accommodation (United Nations, 2020), and there are grave concerns about how this trend will affect social cohesion and equal access to critical public services, including basic healthcare, transport, water and energy. Recent reports suggest that the growth in urban populations will require a $78 trillion infrastructure investment in the coming years (PWC, 2020). Cities consume 75 per cent of the world's natural resources and are responsible for 80 per cent of global carbon emissions (PWC, 2020). Managing the future of urbanisation, including environmental, economic and social sustainability, will be crucial to urban security as we move further into the 2020s.

Cities serve several important political, economic and security functions. They are major economic hubs. The global stock markets are dominated by New York, Hong Kong, London and Tokyo, and they host the global financial infrastructure and institutions that make the global economy run (Statista, 2020). Cities are also major diplomatic hubs, serving global political relationships, with embassies, consulates and myriad private interests circulating for political influence. They have also become important actors in their own right, with a growing agency in international affairs. The ascension of global cities has allowed a range of internationally influential leaders to emerge, from Boris Johnson to Rudy Giuliani; figures who have transcended city politics and built international reputations. Cities have become strategic resources in wars and civil conflicts, too. The 1993 'Black Hawk Down' incident in Mogadishu and the battle for Fallujah in Iraq had major implications for the outcomes of those conflicts and cities have also been sites of major

political transitions such as the Arab Spring which was centred in Tahrir Square in Cairo. Cities also host iconic landmarks such as the Eiffel Tower, Big Ben, One World Trade Center, Sydney Harbour Bridge and Burj Khalifa which have wider political and security significance.

B. The Rise of the Smart City

Smart cities can be defined as those that effectively integrate physical, digital and human systems in urban environments to deliver sustainable, prosperous and inclusive outcomes for their citizens (British Standards Institute, 2014). At present, technology is certainly present in cities, but fully integrated and automated forms of technological governance that connect different services and the people that use them are still under development. Achieving positive outcomes depends on smart city security, and a growing body of literature has emerged addressing the many technological vulnerabilities that appear to be built into smart city projects. The growing dependency of smart cities on technological interconnectivity and data is also increasing their known and unknown vulnerabilities to cyber attacks and threats from foreign hybrid influence. There is a growing literature on the multiple attack surfaces that a smart city grid presents to adversaries and growing concerns over the threats to civil and political rights that they engender (Sookhak et al., 2019). Other scholars have emphasised the security challenges involved, and particularly attacks that cause disruption to services and steal or manipulate the data collected by sensors (Elmaghraby & Losavio, 2014). Smart city infrastructure consists of smart public transport and traffic control, a smart energy grid, smart water supply, smart waste management, smart building operations, smart healthcare, smart delivery systems, smart local governance services, smart back-office systems and others. These smart services are enabled by a synergetic network of physical and virtual infrastructure that redefines how citizens interact with the city and with local governance. 5G networks, the IoT and autonomous service networks and platforms (electronic services that are automated, with humans in-the-loop) are expected to transform and refine smart city design, operations and efficiency as the 2020s unfold. Each of the smart city infrastructure components presents numerous vulnerabilities, but it is the complex, multi-layered and highly interconnected system-of-systems in a smart city infrastructure that is systemically vulnerable to a growing number of threats from cyber crime to hybrid warfare.

At present, there are hundreds of smart city initiatives across the transatlantic area, including iCity in Spain, Triangulum in the UK, and DIMIS in Germany (Nominet, 2018). In 2019, local governments globally spent $95 billion on smart city technologies and global smart city initiative spending is forecast to reach $189 billion by 2023 and $263 billion by 2028 (International Data Corporation, 2020). A simple inventory of the sheer number of municipalities and local governments across Europe offers an even more sobering overview of the scale of the challenge: there are over 87,800 municipalities and local governments in European NATO members and over 88,200 in the EU (vom Howe et al., 2019). These municipalities are home to 74 per

cent of the population in Europe and 82 per cent in North America (United Nations, 2018). The US Department of Transportation has issued a 'Smart City Challenge' and in 2014 the National Institute for Standards and Technology (NIST) launched its Smart Cities and Communities Framework. The European Commission (EC) launched a European innovation partnership on smart cities and communities and since 2017 has spent over €53,5 million on projects addressing the energy, transportation and environmental aspects of smart city grids (EC, 2020a). Already, Europe and North America are home to 26 of the world's largest smart city infrastructures (Eden Strategy Institute, 2018). Europe has the highest density of smart city initiatives (IESE Business School, 2019). A majority of municipalities in the transatlantic area will implement at least some form of smart city infrastructure in the next decade and many such initiatives will increasingly be interconnected across regions and share the same technology, software and hardware in the process. This opens the very real possibility that a successful hack of one such vulnerable system can be replicated en masse, with the help of automated virtual tools to affect multiple cities simultaneously.

3. BRITTLE-AT-THE-MAKING? MAPPING SMART CITY VULNERABILITIES

There is a growing awareness of the cyber security risks embedded in smart city infrastructure and their potential physical effects (US Department of Energy, 2017). Rather than being risk averse, the response framework has been one of risk management (US Department of Homeland Security, 2015). The costs of cyber security for smart city infrastructure between 2020-2024 are projected to grow to over $135 billion (ABI Research, 2019), meaning cyber security design and maintenance becomes comparable to the very development of smart city initiatives. Governments and international organisations in the transatlantic area have developed risk mitigation measures to build 'security by design' into smart city grids. These include a myriad of standardisation and certification schemes, including ISO standards for smart cities (ISO/IEC, 2020), EU certification for ICT devices and services (EC, 2020), the US NIST IoT security requirements (Fagan & Megas, 2020; Singhal, 2020) and NATO telecommunications requirements (NATO, 2019; 2020). There is also specific regulation for critical infrastructure protection, with which national authorities and operators of smart city services all have to comply. Because implementation of these standards and regulations remains a national prerogative, differences in strategic focus, technological capacity and available budgets explain different levels of performance.

Yet, despite these growing investments in cyber security, the threats and vulnerabilities of smart cities are still expanding. Between 2010-2014, the US Department of Energy reported over 1,130 cyber attacks against the national critical infrastructure grid, including 19 against nuclear weapons stockpile facilities; 14 per cent of these attacks were successful, leading to disruption of energy supply services and loss of integrity of the data and industrial

command systems at several facilities (Reilly, 2015). Between 2018 and 2019, there was a 363% increase in the targeting of organisations (including local government entities) by hackers (Malwarebytes, 2019) in a trend that points to a significant shift in the activity patterns of cyber attacks and cyber conflict more broadly, from a focus on attacking individuals towards ever-larger entities, especially organisations and local government entities. This trend of increasingly sophisticated, targeted and widespread cyber-attacks, including against local governance and private industry, is well documented in Europe, too (ENISA, 2020).

Unlike national authorities and large organisations which possess the necessary funding, the technology and, more often, the skilled workforce needed to defend against cyber attacks or comprehensively tackle hybrid warfare campaigns, local governments are far easier targets for technological, social and governance reasons. The systemic approach to the security of smart cities seems to be technologically brittle-by-default, socially brittle-by-nature and politically brittle-by-design.

A. Brittle-by-default? Technological Vulnerabilities of Smart Cities

Smart energy grids and smart water management systems can create security vulnerabilities because they are deployed as a layer over legacy systems with many cyber vulnerabilities that are aggravated by poor maintenance. Some services, for example, use operating systems that have not been updated or patched since the late 1990s or early 2000s, (such as Windows XP, that was exploited during the WannaCry attack) making them easy access points into the smart city grid where hackers can disrupt and corrupt other components. A recent industry report identified 17 distinct 'zero-day' vulnerabilities across four types of smart city systems, eight of which were classified as being of 'critical severity' (Warwick, 2018). While access to these legacy systems is becoming easier, the detection and repair of compromised devices in the network can be extremely challenging and costly (Cerrudo, 2014). For example, detecting a data breach takes on average six months or longer (ENISA, 2020). The multitude of systems, devices and protocols in smart city infrastructure, ranging from Bluetooth to 5G, both software and hardware components, and those produced and operated by a multitude of stakeholders, makes interoperability, coordination and compliance monitoring of common security standards difficult (US Department of Homeland Security, 2015). It also obscures clear lines of responsibility and accountability for failures in the system.

New components and technologies added into smart city networks—such as sensors and IoT devices—continue to be vulnerable, despite the adoption of cyber security standards, safeguards and authentication protocols across the transatlantic area. The focus on increasing broadband access and reducing network latency has led to an increased density of oversubscribed networks, which is particularly relevant in times of crisis when networks experience rapid spikes in data use (Afflerbach, 2020). These networks cannot accommodate all subscribers—people and IoT devices—making them brittle and

prone to failure. Most water and energy contractors have different cyber security protocols and use supervisory control and data acquisition (SCADA), an automation control system that has been proven to be a significant and multi-faceted single point of failure in smart city grids (Kitchin & Dodge, 2017). In a system as interconnected as a smart city, security is a function of its weakest component. As a result of the smart city's high interconnectivity of the data and the systems that run on it, the corruption or disruption of one part of the puzzle has important cascading effects across the entire grid. Jamming and spoofing GPS signals can disrupt critical services such as police, fire, emergency medical services, power grids and financial markets (Polunsky, 2019). These effects can easily be achieved through the use of small commercially available drones.

The market is saturated with producers offering smart city technologies at increasingly affordable prices, which is attractive to local governments whose procurement budgets are under constant pressure. Nevertheless, many producers of smart city technologies lack the experience or best practices on inbuilt cyber security measures in the products they sell. Encryption is rarely a staple of local data (with important implications for privacy and safety) and software is generally used with default cyber security settings still in place. Even where encryption of data could be considered, the widespread deployment of low-power sensors makes their inclusion on an encrypted network link difficult. Local governments generally lack the funding incentives necessary to recruit, train and retain skilled experts to design, operate and maintain their digital critical infrastructure, which leaves open higher risks for human error. A distracted, undertrained or dissatisfied employee can—willingly or not—invite vulnerabilities into the network. As the number of cyber attacks against local entities increases (even more so since Covid-19), phishing emails remain the most widely used tool to gain access into the system. However, new forms of malware and ransomware are also proliferating alongside the malign exploitation of weak personal authentication (Ferbrache, 2020).

Paradoxically, public procurement is still not focusing enough on security-by-design approaches to the technologies and services acquired. Local procurement of new services and technologies may be prioritised because of public visibility gains, despite the high costs, and to the detriment of servicing older systems already deployed in the critical infrastructure grid. For example, a 2018 UK government report estimated the cost of the upgrade of national and local broadband networks to be £33,4 billion over a decade; however, the amount could be 30 per cent lower if authorities gradually upgraded the infrastructure over a longer period (UK NIC, 2018: p. 21). Extended periods of budgetary austerity in the transatlantic area have made long-term local underinvestment in critical infrastructure even more likely. An expected economic downturn as a result of the COVID-19 crisis will incentivise local governments to implement more smart city initiatives while also making more budget savings.

The private sector has led the notable (but also profit-seeking) effort to address technical and cyber security challenges posed by emerging smart city infrastructure. The array of technical solutions includes prioritisation of data security and integrity (especially in the context of 5G networks); failsafe and overriding mechanisms, especially for large-scale command systems; access controls; data encryption; higher IT and cyber security standards and regularly updated security protocols; software patching; the deployment of network intrusion mechanisms; and staff training (Deloitte, 2019). Despite the technological solutions available, cyber or hybrid disruption by state and non-state actors below the use of force and with both military and civilian socio-technological tools rewards the disruptor. It is relatively cheap (ex. dark web ransomware is available for under $50), it provides perpetrators with revenue from, for example, ransomware premiums, and it has public visibility as a result of the days or months-long disruption to local government and public services caused by the attacks (Fernandez et al., 2019). The consequences of cyber attacks on smart city grids have important financial and public trust costs for local governments. Technological vulnerabilities are an important route through which cyber warfare can be instigated, but they are not the only ones. People are the other big part of the smart city puzzle and we discuss this aspect next.

B. Brittle-by-nature? Social Vulnerabilities of Smart Cities

An internet search of 'smart city vulnerabilities' reveals 7,9 million responses, the vast majority of which focus on technical challenges, technical mitigation and technical solutions. Even military literature reveals a predilection with technological challenges and solutions in smart city and urban environments, albeit one that is balanced by practical operational considerations (NATO STO, 2020). The 2018 NATO Capstone Concept on Urban Warfare, for example, includes considerations of the effect the social structure of a city has on the security and success of military operations. Even data privacy literature focuses on the technical rather than the social aspects. Paradoxically, the literature on smart city infrastructure almost entirely avoids considerations of the city's social structure as part of its critical infrastructure, including human behaviours and psychology, challenges related to social cohesion and group identity and issues around social justice and equality. This is an important gap considering that disinformation and 84 per cent of cyber attacks rely on some form of social engineering (ENISA, 2020).

For city inhabitants, the dense smart city infrastructure reconceptualises the city as a 'platform for services' (Kitchin & Dodge, 2018). Local governments provide apps that GPS-track and estimate the arrival time of public transportation (buses, underground, trains), online tax submission, healthcare apps and others. Recent research at Carnegie Mellon University revealed smart city design and operations require more attention to safety, sustainability, equity and resilience. The United Nations (UN) cautions that technological change and smart urbanisation can serve as critical channels for social inclusion, but they can also worsen social exclusion. A city's pre-existing social structure is influential in shaping the impact on smart city infrastructure. Private tech

companies refuse to sell facial recognition technology for smart policing applications used by local law enforcement agencies across the US because the technology is brittle and prone to social biases (Greene, 2020). Less affluent communities cannot afford the skilled work or the investments in modern and secure technologies to safely deploy smart city initiatives, which also increases rather than reduces social exclusion and equitable access to higher standards of living and better local government and public services.

The proliferation of online media as a source of information for an increasing number of people is facilitating the creation of 'echo chambers' for the proliferation of man-made or automated content that spreads disinformation. Cyber warfare and other malign influence campaigns are increasingly sophisticated and exploit local contexts, crises and social tensions. In the age of big data, foreign malign actors need not rely on more than off-the-shelf algorithms that sift through social media and open-source data to reveal several critical indicators for their targeted disinformation campaigns (Hybrid COE, 2020). In this context, big data analysis of Facebook and Twitter posts by a target city's dwellers can reveal their emotions about politically and socially relevant indicators such as elections, political figures, policy priorities or values that, if activated and amplified by disinformation, can undermine and divert democratic processes and institutions. Similar algorithms enable microtargeting of specific categories of a population with highly tailored content that can shape the democratic environment.

The advent of synthetic media, deepfakes and augmented reality tools that can already realistically portray real political leaders saying or doing things that they have never in reality done adds a layer of complexity to the human, behavioural and social challenge created by emerging technologies. This challenge is all the more concerning in dense urban areas, such as smart cities, where information overload and the inability of local governments to fully shape and control their information environments is a serious vulnerability.

Social disorder can be amplified faster today through malign hybrid influencing. Synthetic media with wide and rapid dissemination across dense information networks of smart cities can lead to significant and rapidly escalating social disorder. Because the nature of online communities is not geographically contiguous and urban populations share frustrations over aspects of local governance, smart city social tensions over real or doctored content and deepfakes have a great potential for contagion. As recent research shows, deepfakes and synthetic media are more likely to be deployed in a targeted manner such as during a crisis to maximise impact while avoiding detection, mitigation and attribution (Hwang, 2020).

The social, physical and virtual infrastructure in a smart city meets in another important domain—namely, the symbolism of specific city locations for political and social movements. Social geography is a well-studied factor that shapes urban environments and smart cities contribute to the creation

of urban social geography at scale. Places like Tahrir Square in Cairo, Tiananmen Square in Beijing, University Square in Bucharest, Maidan Square in Kiev and, more recently, Lafayette Square in Washington DC and the Justice Center area in Portland carry much social symbolism associated with the popular struggle against perceived national or local government abuse of power. The symbolism around city landmarks can also be an important trigger of social disorder, including during the Bronze soldier incident in Estonia in 2007.

Social disorder can also follow urban economic downturns, as seen in the massive protests against austerity across Greece. As in our scenario at the beginning of the article, inequities in cities and disparities in living standards can be extreme and be exploited by malicious actors. Global urban centres generate 80 per cent of global GDP (World Bank, 2020). A recent report showed smart city initiatives increased local economic growth by 21 per cent in 136 cities across the world (ESI ThoughtLab, 2020). The implementation of smart city infrastructure facilitated by technological innovations in 5G, big data, AI, robotics and IoT is also set to change patterns of urban economic activity (ex. automation), which will trigger short and longer-term changes in the city's socio-economic structure. Technological change could increase social exclusion through job polarisation, wage inequality and unequal access to public services particularly in large urban areas (UNDESA, 2020).

Privacy concerns and the integrity of personal data are just part of the debate over smart cities and a key part of the intersection between technological vulnerabilities and human-centred and societal dynamics, including societal security dilemmas where citizens fear other groups or their governments. With over 850 zettabytes of data created by over eight billion IoT devices in 2021 alone, the information contained by this largely unstructured and uncured data could reveal important insights for national governments and adversaries alike. Approximately 40 per cent of cities currently use predictive data, and the number of smart cities, volume and types of data (particularly AI-generated, geospatial and behavioural data use) are expected to grow exponentially over the coming years (ESI ThoughtLab, 2020: p. 23). Smart cities will channel and process huge amounts of private-individual and commercial-industrial data, both of which require increased security. A data breach that leads to widespread loss of private user data or proprietary industrial data can have significant local and national economic security implications by exposing industrial vulnerabilities, secrets or leading to a loss of economic competitiveness. This is a particularly significant security concern in Europe, which owns the world's largest volume of industrial data.

While cyber security threats to smart cities are evolving, the 'attack surface' of information warfare is likely to continue to include humans and machines. Unless a comprehensive systemic approach to smart city security is adopted to include its most valuable component—people—hybrid warfare campaigns will continue to undermine local government and security across the transatlantic space. Societal resilience is not a uniquely national-level construct—in fact, much of it begins from the bottom up and local governments,

particularly in the context of smart cities, as increasingly important actors in this process. Perhaps the way to refocus the narrative about the security of smart cities is to comprehensively redefine smart cities as synergetic and integrated physical, virtual and human components, structures and systems.

C. Brittle-by-design? The Missing Link Between Smart City and National Security

One aspect that is virtually absent from the literature on smart cities is their relationship to broader national security considerations and national and international politics, including crisis management. While local government entities are increasingly an appealing, albeit incidental target for cyber criminals driven by vulnerabilities rather than political motivations against specific cities, smart cities could increasingly present more attractive and easier targets for state adversaries or state-supported cyber criminals for disruption and destruction. Large smart city infrastructures like London, Paris and Amsterdam are critical parts of the national security grids and fundamental to economic security. Prolonged mass disruption of their infrastructure—as has been recently seen in the case of month-long disruption in public services as a result of cyber attacks against American municipalities (Robles, 2020)—would be a serious national security threat to allied nations.

This is in part a result of the lesser-known nature of the complex interdependencies and politico-administrative between the levels of local and national governance (Hybrid CoE, 2020). Recent research has revealed the high dependency of critical smart city infrastructure on services generally coordinated at the national level, including satellite-based services, GPS and 5G mobile networks. Despite the dependency of local government daily operations on such technologies, policy-making processes rarely if ever include local government representatives (Polunsky, 2019).

Lessons learned in the field of cyber security are already being broadened and applied in relation to local government and the security of smart city infrastructure, but greater cooperation is needed on lessons learned between local and national government, including relating to information-sharing on evolving cyber threats. The availability of national-level guidance on safety standards and protocols, the presence of local government representatives in national decision-making bodies on vital components of critical infrastructure—including critical infrastructure around democratic processes and institutions such as elections—and the establishment of flexible governance structures will become a prerequisite in ensuring the resilience and security of smart cities across the transatlantic area. In this respect, our argument is not that the national military should be more involved in the governance of cities, but that local government officials and processes should be better integrated into national decision making and security planning.

One urgent area to address is the clarification and exercise of clear roles and responsibilities for the secure operation of smart city infrastructure and for the response to a variety of types of events of varying scopes in relation to smart city infrastructure. There are national and supranational regulations

(EU and NATO) in place for the protection of critical infrastructure which encompasses national, federal and local authorities and private enterprises. Nevertheless, looking towards the future when hybrid and cyber threats will target the seam between the responsibilities of different national, local, governmental and private actors, further clarification and constant updating of these specific roles is required to avoid grey areas of responsibility.

Local threat mapping can be more complex than at the national level and growing cyber attacks against local government entities can make it difficult for local officials to see the bigger picture of hybrid influence campaigns. Local governments face more challenges in linking local effects and events with global competition dynamics, and often do not have the budgets, knowledge, resources or remits to do so. Facilitating deeper vertical (national-to-local) and horizontal (local-to-local) cooperation on best security practices for smart city infrastructure and for the response to events targeting smart city grids, information sharing, audits and the training and exercising of personnel—including contractors and private industry—would be essential steps towards enhancing the preparedness and resilience of smart city environments. This could involve a cyber security committee or advisory group staffed by representatives from the national security services, local government, police and tech sector, tasked with coordinating responses to major cyber incidents, or indeed a multi-stakeholder and municipality information sharing and analysis centre. Recent tensions between the City of London and the Johnson government over COVID-19 responses and the lack of City representation on the government's national emergency management committee are illustrative of the inherent political challenges here (O'Reilly, 2020).

Finally, why should an international alliance like NATO be concerned with smart city security? While sub-national security preparedness is a national responsibility, NATO decisions bear an indirect but critical role in how smart cities conceptualise and design their security architectures. For example, in December 2019 NATO updated its baseline security requirements for telecommunications systems, including 5G networks (NATO, 2019). National governments are principally responsible for the implementation of such requirements, but so are local governments. Yet national policies on telecommunications networks are made with little to no participation or input from local governments and private industry who are subject to said legislation. Smart city infrastructure threats can create important second and third-order effects for the national and alliance levels of governance. For example, cyber attacks on critical infrastructure that lead to man-made disasters such as floods or fires can divert the military capabilities needed for alliance missions over long periods. Alternatively, such events can disrupt military planning, including military mobility, or the operation of militarily relevant infrastructure and logistical hubs. Particularly in areas with greater local autonomy, uncoordinated local government decisions could create vulnerabilities that are less visible because of the lack of clarity over the relationships between security architectures at national and local levels, but that could nevertheless be systematically or opportunistically exploited by adversaries.

NATO Science and Technology Organization's (STO) 2020 Report on Science and Technology trends refers to smart cities as 'synergistic systems' that have critical consequences for the Alliance's ability to defend allied territory or engage in urban warfare beyond the transatlantic area (NATO STO, 2020). Unsurprisingly, the main preoccupation with urban environments in NATO is on the operational side. However, NATO and national military infrastructure largely rely on local public services and grids. Much can be done on improving the preparedness of local governments to withstand severe hybrid and cyber attacks on smart city infrastructure and prevail, whether the use of force is necessary or not. Venues like the NATO Parliamentary Assembly, NATO and EU Centres of Excellence and Atlantic Associations, but also engagement with local governance networks could help assist local and national governments and the Alliance, including by encouraging an acceleration across the transatlantic area of local government-oriented resilience and preparedness-enhancing measures.

4. CONCLUSION

The paper has argued that smart cities present a very real local challenge to national and international security policy at the technological, social and political governance levels. Cyber warfare, internet-enabled attacks by states against critical infrastructure and the malicious exploitation of information networks will target cities and their increasing connectivity. Such campaigns will have both political and social effects, including exacerbating identity divides, sowing division and eroding trust in governance systems and elected officials. The focus on technological solutions for smart city security obscures the adaptations needed in the broader local and national security ecosystem. The NATO 2030 reflection process presents a clear opportunity to think more deeply about the implications of local governance on the Alliance's ability to operate smoothly and efficiently in the coming decade. Continuing to build vertical and horizontal cooperation between local, national and allied security planning should be foregrounded in this process as a way of avoiding building brittle security structures.

5. REFERENCES

ABI Research. (2019) Lack of Critical Infrastructure Cybersecurity Investments in Smart Cities will Seed the Future IoT Vulnerabilities. Available from: https://www.abiresearch.com/press/lack-critical-infrastructure-cybersecurity-investments-smart-cities-will-seed-future-iot-vulnerabilities/ [Accessed 4th August 2020].

Afflerbach, A. (2019) Broadband Performance is About More than Speed, *CTC Technology*, available from: https://www.ctcnet.us/blog/broadband-performance-is-about-more-than-speed/ [Accessed 30th October 2020].

Alderson, A.S., et al. (2006) Globalization and the world city system: Preliminary results from a longitudinal dataset. In Taylor, P.J. et al. (eds.) *Cities in glo-*

balization: Practices, policies and theories. London, Routledge, pp. 21-36.

Barnes, C. & Barraclough, T. (2020) Deepfakes and synthetic media. In Steff, R., Burton, J. & Soare, S.R., *Emerging technologies and international security: Machines, the state, and war*. London, Routledge, pp. 206-220.

British Standards Institute. (2014) *PAS 181 Smart city framework*. Available from: https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-181-smart-cities-framework/ [Accessed 28th August 2020].

Buzan, B. (2007) *People, States and Fear* (ECPR classics). Colchester, European Consortium for Political Research.

Cerrudo, C. (2014) Hacking US Traffic Control Systems. *Defcon Conference* presentation. Available from: https://www.defcon.org/images/defcon-22/dc-22-presentations/Cerrudo/DEFCON-22-Cesar-Cerrudo-Hacking-Traffic-Control-Systems-UPDATED.pdf [Accessed 8th August 2020].

Deloitte Center for Government Insights. (2019) Making smart cities cybersecure. Available from: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Report_making_smart_cities_cyber_secure.pdf [Accessed 10th August 2020].

Eden Strategy Institute. (2018) *Top 50 Smart City Governments*. Available from https://static1.squarespace.com/static/5b3c517fec4eb767a04e73ff/t/5b513c57aa4a99f62d168e60/1532050650562/Eden-OXD_Top+50+Smart+City+Governments.pdf [Accessed 8th August 2020].

Elmaghraby, A.S., and Losavio, M. (2014) Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*. 5 (4), 491-497.

ESI ThoughtLab. (2020) Smarter Cities 2025 Building a Sustainable Business and Financing Plan. Available from: https://econsultsolutions.com/wp-content/uploads/2018/11/ESI-ThoughtLab_Smarter-Cities-2025_ebook_FINAL.pdf [Accessed 10th August 2020].

European Commission. (2020a) *EU-funded projects on Smart Cities*. Available from: https://ec.europa.eu/digital-single-market/en/eu-funded-projects-smart-cities [Accessed 28th February 2020].

European Commission. (2020b) The EU cybersecurity certification framework. Available from: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework [Accessed 16th October 2020].

European Commission. (2017) The making of a smart city: best practices across Europe. Available from: https://smartcities-infosystem.eu/sites/default/files/document/the_making_of_a_smart_city_-_best_practices_across_europe.pdf [Accessed 10th August 2020].

European Union Agency for Cybersecurity. (2020) ENISA Threat Landscape 2020. Available from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents [Accessed 29th October 2020].

Hybrid COE (The European Centre of Excellence for Countering Hybrid Threats). (2020) Helsinki in the era of hybrid threats – Hybrid influencing and the city. Available from: https://www.hybridcoe.fi/wp-content/uploads/2018/08/Helsinki-in-the-era-of-hybrid-threats---Hybrid-influencing-and-the-city_ENG.pdf [Accessed 4th August 2020].

Fagan, M.J., Megas, K.N. et al. (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. Available from: https://www.nist.gov/publications/foundational-cybersecurity-activities-iot-device-manufacturers [Accessed 16th October 2020].

Ferbrache, D. (2020) The rise of ransomware during COVID-19, KPMG. Available from: https://home.kpmg/xx/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html [Accessed 30th October 2020].

Fernandez, M. et al (2019) Ransomware Attack Hits 22 Texas Towns, Authorities Say. *New York Times*, 20 August. Available from: https://www.nytimes.com/2019/08/20/us/texas-ransomware.html [Accessed 8th August 2020].

Greene, J. (2020) Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM. *Washington Post*, June 11. Available from: https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ [Accessed 12th June 2020].

Hwang, T. (2020) Deepfakes: A Grounded Threat Assessment. *Centre for Security and Emerging Technologies, Georgetown University*. Available from: https://cset.georgetown.edu/research/deepfakes-a-grounded-threat-assessment/ [Accessed 10th August 2020].

IESE Business School. (2019) These Are the Smartest Cities in The World For 2019. Available from: https://www.forbes.com/sites/iese/2019/05/21/these-are-the-smartest-cities-in-the-world-for-2019/#606301461429 [Accessed 8th August 2020].

IESE Business School. (2019) IESE Cities in Motion Index 2019. Available from: https://media.iese.edu/research/pdfs/ST-0509-E.pdf [Accessed 10th July 2020].

International Data Corporation. (2020) *Smart Cities Initiatives Forecast to Drover $189 Billion in Spending in 2023*. Available from: https://www.idc.com/getdoc.jsp?containerId=prUS45303119 [Accessed 14th August 2020].

International Organization for Standardization. (2020) *ISO/IEC 30145-3:2020 Information technology — Smart City ICT reference framework — Part 3: Smart city engineering framework.* Available from: https://www.iso.org/standard/76373.html [Accessed 16th October 2020].

Kitchin, R. & Dodge, M. (2017) The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*. 26 (2), 47-65, DOI: 10.1080/10630732.2017.1408002.

Malwarebytes. (2019) Malwarebytes Reports 365 Percent Spike in Business Ransomware Detections. Available from: https://press.malwarebytes.com/2019/08/08/malwarebytes-reports-365-percent-spike-in-business-ransomware-detections/#:~:text=Overall%20ransomware%20detections%20against%20businesses,ransomware%20as%20a%20major%20contributor [Accessed 8th August 2020].

OECD. (2018) Smart Cities and Inclusive Growth. Available from: https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf [Accessed 12th August 2020].

O'Reilly, L. (2020). Sadiq Khan says Cobra hasn't met since May 10 and he hasn't spoken to Boris Johnson in four months. *Evening Standard*. Available from: https://www.standard.co.uk/news/politics/sadiq-khan-cobra-boris-johnson-may-10-a4550651.html [Accessed 30th October 2020].

NATO. (2020) *Resilience and Article 3*. Available from: https://www.nato.int/cps/en/natohq/topics_132722.htm [Accessed 16th October 2020].

NATO. (2019) NATO Defence Ministers to address key issues for the Alliance. *Press Release.* Available from: https://www.nato.int/cps/en/natohq/169941.htm?selectedLocale=en [Accessed 16th October 2020].

NATO Science & Technology Organization. (2020) Science & Technology Trends

2020-2040: Exploring the S&T Edge. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf [Accessed 30th March 2020].

Nominet. (2018). Smart city projects showcase – great uses of IoT in urban contexts, available from: https://www.nominet.uk/smart-city-projects-showcase-great-uses-of-iot-in-urban-contexts/ [Accessed 30th October 2020].

Polunsky, S. (2019) The City-Sized Hole in U.S. GPS Planning. *Belfer Center, Harvard University Kennedy School*, Homeland Security Policy Paper #3. Available from: https://www.belfercenter.org/sites/default/files/files/publication/HSP%20paper%20series%203%20-%20draft%202.pdf [Accessed 10th August 2020].

PWC. (2020) *Rapid Urbanisation*. Available from: https://www.pwc.co.uk/issues/megatrends/rapid-urbanisation.html [Accessed 14th August 2020].

Reilly, S. (2015) Records: Energy Department struck by cyber-attacks *USA Today*. Available from: https://eu.usatoday.com/story/news/2015/09/09/cyber-attacks-doe-energy/71929786/ [Accessed 10th August 2020].

Ritchie, H. & Roser, M. (2018) *Urbanisation*. Our World in Data. Available from: https://ourworldindata.org/urbanization [Accessed 8th August 2020].

Robles, F. (2019) A City Paid a Hefty Ransom to Hackers. But Its Pains Are Far From Over. *New York Times*, 7 July. Available from: https://www.nytimes.com/2019/07/07/us/florida-ransom-hack.html?action=click&module=RelatedLinks&pgtype=Article [Accessed 7th August 2020].

Smart Cities World. (2019) *Smart city technology market to grow to $263 billion by 2028.* Available from: https://www.smartcitiesworld.net/news/news/navigant-tracks-smart-city-projects-around-the-world-4296 [Accessed 8th August 2020].

Singhal, A., Ibrahim, K., Majumdar, S., & Bastos, D. (2020) Defining Actionable Rules for Verifying IOT Safety and Security. Available from: https://www.nist.gov/publications/defining-actionable-rules-verifying-iot-safety-and-security [Accessed 16th October 2020].

Sookhak, M., Tang, M., He, Y., & Yu, R.F. (2018) 'Security and privacy of smart cities: a survey, research issues and challenges.' *IEEE Communications Surveys & Tutorials*. 21 (2), 1718-1743 [Accessed 16 October 2020].

Statista. (2020) *Distribution of countries with largest stock markets worldwide as of January 2020*. Available from: https://www.statista.com/statistics/710680/global-stock-markets-by-country/ [Accessed 30th September 2020].

United Kingdom National Infrastructure Commission. (2018) National Infrastructure Assessment Report. Available from: https://www.nic.org.uk/wp-content/uploads/CCS001_CCS0618917350-001_NIC-NIA_Accessible.pdf [Accessed 14th August 2020].

United Nations. (2020) *Sustainable Cities and Communities*. Available from: https://unstats.un.org/sdgs/report/2019/goal-11/ [Accessed 8th August 2020].

United Nations. (2018) *68% of the world population projected to live in urban areas by 2050, says UN*. Available from: https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html [Accessed 8th August 2020].

United States Department of Energy. (2017) Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities. Available from: https://www.energy.gov/sites/prod/files/2018/05/f51/EO13800%20electricity%20subsector%20report.pdf [Accessed 20th August 2020].

United States Department of Homeland Security. (2015) The Future of Smart Cities:

PART III:
Warfighting, the Cyber Domain and NATO's Response

Cyber Threats to NATO from a Multi-Domain Perspective

James Black
Research Leader
Defence, Security and Infrastructure
RAND Europe

Alice Lynch[1]
Former Security and Defence Analyst
RAND Europe

Abstract: This paper situates cyber threats within the wider context of a continued shift towards multi-domain concepts by NATO Allies and adversaries alike. These emerging concepts emphasise the importance of integration for achieving advantage; however, with greater connectivity and network-dependency comes greater potential vulnerability and consequences from disruption. This paper considers challenges associated with closer integration within and across military domains and examines how potential adversaries (Russia and China) are embracing variations on multi-domain and systems thinking and prioritising offensive cyber capabilities to exploit seams and vulnerabilities to disorientate, paralyse and demoralise NATO in any future conflict. Acknowledging that cyber attacks do not exist in a vacuum, this paper places discussions of cyber threats in the context of how the Alliance plans to operate, fight and win in future competition and conflict. In doing so, it highlights the adversary's perspective on how, when and why it might employ cyber capabilities to gain an advantage over NATO forces. The paper then considers the implications for NATO in terms of internal barriers, limitations and vulnerabilities that challenge the Alliance's ability to respond to these threats. Improved understanding of the interlinkages between these external threats and internal vulnerabilities is essential in achieving the genuine and wide-reaching transformation required for the Alliance to bolster its cohesion, improve its strategic resilience and ensure its ability to realise its ambitions in cyberspace and across all domains.

Keywords: *Cyber, multi-domain, cross-domain, concepts, Russia, China*

[1] Disclaimer: Alice Lynch has contributed to this paper in a personal capacity, and the analysis and views expressed therein do not necessarily reflect those of her current employer.

1. INTRODUCTION

Fully understanding future cyber threats to the North Atlantic Treaty Organisation (NATO) necessitates looking beyond trends in cyberspace and considering how these both shape and are shaped by threats in or across other operational domains. NATO, the US and other Allies are increasingly developing concepts, forces and capabilities that go beyond the traditional focus on 'joint' to embrace ambitious visions for future multi-domain operations (MDO). Adversaries are similarly developing and employing cyber capabilities against the Alliance not as part of some segregated cyberwar, but rather as critical integrators and enablers of their own variations on MDO and systems thinking.

This paper situates cyber threats in the wider context of this evolving MDO theory and practice. First, it introduces the logic and focus of emerging US and NATO concepts for multi-domain and how cyberspace fits within them. Second, it examines cyberspace's evolving role in the multi-domain thinking of Russia, China and, to a lesser extent, Iran and the Democratic People's Republic of Korea (DPRK), recognising that NATO can only truly mitigate threats if it understands potential adversaries in terms of both capability and intent. Lieutenant General Thomas J. Sharpy of Allied Command Transformation (ACT) warns that NATO otherwise risks MDO being the 'Sputnik moment of this generation', as adversaries increasingly combine cyber, space, electronic and information warfare capabilities to exploit seams in Alliance decision-making and joint operations (Sharpy, 2020). Third, this paper considers the internal challenges and vulnerabilities NATO faces in adapting to future cyber and multi-domain operations.

Collectively, the sections of this paper underscore the need for genuine and wide-reaching transformation if the Alliance is to bolster its cohesion, improve its strategic resilience and ensure its ability to compete in cyberspace and across all domains.

2. CYBER AS AN OPERATIONAL DOMAIN

NATO's contemporary strategic environment is characterised by continuous global competition, both above and below the threshold of armed conflict. Potential adversaries are closing the gap; NATO's competitive edge has been eroded in every military domain, across air, land, sea, space and cyberspace (Knighton, 2019). Rapid technological developments exploiting cyberspace and the electromagnetic spectrum (EMS) present the Alliance with new challenges as threats from increasingly sophisticated adversaries become more complex, destructive and unpredictable (Brent, 2019). Accordingly, the Allies have sought to operationalise cyberspace. At the 2016 Warsaw Summit, they formally recognised cyber as an operational domain, alongside air, land,

maritime and, since 2019, space (NATO, 2020a; NATO, 2020b).[2] This was followed in 2018 by establishment of a Cyberspace Operations Centre (CyOC) as a new NATO theatre component command, with plans to reach full operating capability by 2023 (Brzozowksi, 2018; Brent, 2019). At the 2018 Brussels Summit, Allies issued a joint declaration that 'we must be able to operate as effectively in cyberspace as we do in the air, on land, and at sea to strengthen and support the Alliance's overall deterrence and defence posture' (NATO, 2018a).

Efforts to operationalise the cyber domain include recently published doctrine. *AJP-3.20 Allied Joint Publication Doctrine of Cyberspace Operations* sets out the principles by which joint cyber operations may be planned, executed and assessed (NATO, 2020c). This reflects a shift away from understanding cyber as an enabler of operations in other domains towards being a domain in its own right through which deterrence and coercion can be practised and decisive kinetic and non-kinetic effects delivered (Shea, 2018).[3] However, cyberspace does not exist in a vacuum. Viewing it as a solitary fifth domain risks underestimating the full implications of cyber threats' convergence with those emerging from other domains, thereby undermining the ability to deter and defend against adversaries exploiting seams and vulnerabilities within the increasingly interconnected systems, infrastructure and processes of NATO and individual Allies.

A. Situating the Cyber Domain within Multi-Domain Thinking

Technology is facilitating unprecedented integration across and between domains as military platforms and systems increasingly form part of a complex, networked ecosystem or system-of-systems' (NATO, 2018b).[4] Cyber-related developments are therefore increasingly understood in the context of interlinkages and 'convergence'[5] across domain boundaries, most prominently within emerging US concepts of MDO (TRADOC, 2018).

Much of today's multi-domain thinking can be traced back to concepts of AirLand Battle developed by the US Army in the 1970s and 1980s. AirLand Battle sought to deepen the coordination of manoeuvring land forces and airpower, leveraging satellite technology, theatre battle networks and precision-guided munitions to counter the Warsaw Pact's numerical superiority in the European theatre (Manea, 2018). Central to AirLand Battle were the

[2] Though NATO now formally recognises five operating domains, notably there is no commonly agreed upon definition of 'domain' within the Alliance. See: Donnelly & Farley, 2019.

[3] NATO does not intend to develop its own offensive cyber capabilities; however, individual Allies have agreed to integrate national capabilities into NATO missions. See: Tucker, 2019.

[4] Systems-of-systems are a 'set or arrangement of systems that results when independent…systems are integrated into a larger system that delivers unique capabilities.' See: DAU, 2020.

[5] Convergence can be defined as 'the integration of capabilities across domains, environments, and functions in time and physical space to achieve a purpose'. See: TRADOC, 2017.

concepts of 'Integrated Battle' and the 'Extended Battlefield'. Integrated Battle stipulated that every asset of the air-ground team at a commander's disposal should be employed together to defeat the opponent. Extended Battlefield involved attacking all echelons of the opponent's formations simultaneously (Johnson 2018). AirLand Battle remained primarily focused on the air and land domains. 'Cyberspace' was not yet understood as a domain in its own right, although strong emphasis was placed on computer networks as an enabler and force multiplier for joint operations. Many of AirLand Battle's core principles endured and evolved to guide the development of 'network-centric warfare' in the 1990s and 2000s, influencing current NATO doctrine on joint operations and, more recently, shaping the multi-domain thinking now so prominent in the US and increasingly among NATO Allies.

While MDO originates from US Army thinking, others have begun developing their own variations, including: the US Air Force's Multi-Domain Command and Control; recent US joint terminology of Joint All-Domain Operations; Norway's Holistic Operations; and the UK's Multi-Domain Integration (Watling & Roper, 2019; Carter, 2019; Underwood, 2020). While these all refer to similar fundamental principles, NATO has no unifying definition of MDO and differences persist even between US service branches (Grest & Heren, 2019). This paper assumes a generic use of the term MDO to encompass these various still-evolving concepts and its use does not specifically endorse those of any single service or nation.

MDO is premised on the notion that deeper integration within and across domains will enable NATO to overcome adversary strategies and capabilities aimed at preventing access to theatres of operations and limiting freedom of manoeuvre, often referred to in the West—though not, notably, in Russian or Chinese literature —as Anti-Access/Area-Denial (A2/AD). Given technological developments and growing independencies across domains, previous concepts of 'jointness' are no longer seen as sufficient to address such threats or to reflect the importance of new cyber and space capabilities (Siegemund, 2018).

The primary purpose of MDO, therefore, is to prepare for future integrated operations across the full spectrum of conflict by removing the institutional segregation of military capabilities and elevating the role of service branches and domains typically thought of as support (Freedberg, 2018). In contrast with joint warfare which remains premised on separate domains in which operations are principally led by one service and where capabilities in one domain are used to support those in another, MDO presents a more ambitious vision genuinely agnostic of domain boundaries or traditional force structures (Perkins & Andera, 2018). Harnessing synergies across cyberspace, space and the EMS, MDO enables commanders to orchestrate and converge effects at the optimal tempo in windows of opportunity, thus '[presenting] the enemy with multiple dilemmas across multiple domains and in multiple locations' (Feickert, 2020: p. 2). This emphasises integration as key to gaining an advantage in future conflicts in which adversaries contest

NATO in all domains with the convergence of networked sensors and effectors in different domains producing an overall effect greater than the sum of its parts (Lindsay & Gartzke, 2020; Siegmund, 2018).

B. Emerging Multi-Domain Concepts within NATO

While high-level principles of US MDO are maturing, the specifics of how to operationalise them remain a work-in-progress (Clare, 2020). Nonetheless, several other Allies have begun exploring similar concepts. The Tri-lateral Strategic Steering Group comprising the US, UK and France has investigated Multi-Domain Warfare (MDW) based on shared recognition that future adversaries will combine conventional, asymmetric and hybrid capabilities and tactics across all domains (Perkins & Olivieri, 2018). The UK's own Multi-Domain Integration (MDI) concept adopts a similar rationale to that of the US, aiming to 'achieve the seamless planning and execution of activities and effects across all domains at a pace and tempo that outstrips our adversaries' (Barry, 2020) to gain information advantage; key priorities being to extend joint operations into cyberspace and exploit data and networks more effectively.

NATO is also beginning to consider implications for implementing MDO at the Alliance level, especially around interoperability and command and control (C2). For example, the NATO Command and Control Centre of Excellence (NATO C2COE) has made MDO the focus of its annual seminar for 2020 (NATO C2COE, 2020b); while the Joint Air Power Competence Centre is investigating ramifications for C2 and future airpower (Harrigian, 2020). The NATO Science and Technology Organisation (STO) also has projects focused on agile multi-domain C2 and wargaming MDO in an A2/AD environment (NATO STO, 2018; NATO STO, 2020). Multi-domain thinking was also evident in Exercise *Trident Juncture 2018* (TRJE18), which incorporated a robust opposition space force order of battle and cyber capabilities in its scenario development. With experimentation efforts ongoing to develop a new *NATO Warfighting Capstone Concept* (NWCC) looking out to a 20-year horizon, Supreme Allied Commander Europe (SACEUR) has also stipulated that high-intensity, near peer-to-peer, multi-domain scenarios should be the main priorities for future NATO training, exercises and force development (NATO, 2020d; NATO2020e; Wijninga, 2019).

C. Recognising Cyberspace as Both an Opportunity and Risk for MDO

Networks enable collection, communication and consolidation of data across organisations, commands and domains; accordingly, cyberspace enables manoeuvre[6] across all domains (Conti & Raymond, 2017). It extends the reach of operations into the 'strategic support area' and the homeland, while offering alternatives to kinetic effects (TRADOC, 2018; Lindsay & Gartzke, 2020). Cyber operations also create windows of opportunity for action in other domains, providing commanders with a broader range of options

[5] Manoeuvre aims 'to gain positional advantage in respect to the adversary from which force can be threatened or applied [...] manoeuvre is the means by which a commander sets the terms in time and space, declines or joins combat or exploits emerging developments.' See: NATO, 2019b: p. 21).

to exploit adversaries' vulnerabilities as they emerge, rather than being restricted to siloed force constructs and physical sensors and effectors (Nakasone & Lewis, 2017; NATO, 2020c).

While employing cyber capabilities as an integrated part of MDO may enhance NATO's combat effectiveness, it may also create new vulnerabilities. These arise from dependency on connectivity and data within an increasingly complex system-of-systems (Joiner & Tutty, 2018). NATO's adversaries may identify and exploit existing vulnerabilities in military platforms and networks or create new ones through, for example, cyber espionage and the manipulation of technology supply chains and markets (Conti & Fanelli, 2019). These create windows of opportunity for adversaries to undermine NATO's cyber defences or to compromise the cybersecurity of governments, industry and critical national infrastructure, shaping political, strategic and operational outcomes across all domains through hostile action in cyberspace (Schneider, 2019).

Activities in cyberspace and the EMS are therefore key enablers for MDO, but also areas of risk. Effective integration within and across nations, services, commands and domains is impractical without secure and resilient lines of communication; in short, success within a multi-domain environment cannot be achieved without the interconnected networks and secure systems constituting the base of the cyber domain (Shea, 2018; Zadalis, 2018). There is also an increasing overlap between cyber threats and space. As C2 systems increasingly rely on space to gather and disseminate mission-critical data, any cyber, jamming, spoofing or physical attack on satellites or ground stations could have cascading effects across all domains and on strategic weapon systems and early warning (Unal, 2019).

D. Adversary Perspectives

NATO's adversaries have explicitly recognised the vulnerabilities inherent in the Alliance's growing dependence on networks, cyberspace, satellite technologies and the EMS. They now seek to exploit these vulnerabilities through their own variations on multi-domain concepts (Nakasone & Lewis, 2017; Schneider, 2019). NATO Allies are not alone in adopting a multi-domain understanding of the future battlespace. While not explicitly embracing the lexicon of US MDO, adversaries nonetheless express similar themes in their own languages. These emerging concepts are increasingly made manifest through joint operations, investment priorities and force and capability development initiatives. This section examines how selected non-NATO nations, principally Russia and China, are approaching multi-domain thinking in theory and in practice. It also considers how each is integrating the cyber domain into its systems thinking, providing an understanding of how cyber threats to NATO are evolving both in terms of hostile intent and capability.

1) Russian Federation

Cyberspace forms part of Russia's strategy of harnessing multi-domain synergies through its interrelated concepts of 'new-type war', 'reflexive con-

trol' and 'disorganisation', which together seek to create strategic conditions for prevailing over the US and NATO. Russian doctrine, activities, force structures and capability development efforts indicate that Moscow is refining and beginning to implement variations on multi-domain thinking. Observing the evolution of network-centric warfare within NATO since AirLand Battle, Russia is seeking to leverage synergies across physical and virtual domains to contest NATO above and below the threshold of armed conflict, creating favourable conditions to seize the advantage in the initial period of war (IPW) (Greisemer, 2018).[7] To achieve this, Russian doctrine emphasises exploiting new technologies and asymmetric means to counter perceived Western advantages, highlighting opportunities arising from cyberspace, alongside the electronic, information and space domains. This asymmetric thinking is expressed through Russia's concept of 'new-type war', which focuses on integration across domains to achieve information superiority and shape strategic conditions through 'reflexive control'.

Reflexive control is the practice of manipulating the adversary's perceptions and decision-making processes through the deliberate construction of information flows to deceive, persuade, coerce and otherwise influence the opponent (Adamsky, 2015). This seeks to exploit NATO's weaknesses with minimal use of kinetic force, achieving maximum effect with minimal use of Russia's resources (Galeotti, 2016). Reflexive control is employed in conjunction with the interrelated concept of 'disorganisation', a strategy of disrupting or degrading an opponent's C2 networks to hinder their ability to coordinate or integrate across multiple domains, thus providing Russia with decision advantage and increased likelihood of victory (Adamsky, 2015).

Cyberspace is viewed as an important enabler, integrator and multiplier. Within 'new-type war', the information domain and exploitation of cyberspace and the EMS are viewed as the means through which Russia can achieve cross-domain synergy and exercise reflexive control creating time, space and manoeuvre advantage for Russian forces while disorganising NATO. For example, during sub-threshold operations or in the IPW, cyber espionage can elicit valuable intelligence on adversary operations in other domains and during operations, targeted cyber attacks can disrupt the adversary's networked C2 systems. At the strategic level, cyber activities support information operations to confuse, influence or mislead target audiences and undermine NATO's cohesion and will-to-fight (Sprang, 2018). Cyberspace thereby provides new methods for disrupting and degrading NATO's networked information and communication systems to achieve Russia's operational and strategic objectives within and across multiple domains (Kilcullen, 2020).

Recent Battalion Tactical Group (BTG) operations in Ukraine provide practical examples of how Russia seeks to exploit cyberspace to operationalise

[7] Russia's IPW concept recognises readiness and will-to-fight as key determinants of conflict outcomes, with early, swift and devastating action potentially decisive. Today, Russian understanding of the IPW emphasises cyber-attacks and broader information operations to degrade the adversary's C2. See: Thomas, 2019.

its own variation on multi-domain concepts (Sprang, 2018). Within Russia's new integrated approach to warfare, BTG commanders are provided with capabilities across domains to achieve a specific operational effect. This includes enablers such as EMS capabilities, previously siloed within what used to be an inflexible force structure (Griesemer, 2018). In multiple confrontations with Ukrainian forces,[8] Russia deployed cyber capabilities in concert with other weapons spanning the domains including uncrewed aerial systems (UAS) and ground forces under a single battalion commander. To achieve a combined effect, Russian forces first disrupted Ukrainian communications and decision-making through targeted cyber-attacks and jamming. With Ukrainian C2 compromised, UAS conducted detailed reconnaissance and target acquisition against Ukrainian positions, enabling devastating long-range rocket and tube artillery strikes (Griesemer, 2018).

Russia has also made tactical use of cyber, electronic and information warfare alongside conventional forces to achieve multi-domain effects in Syria, both targeting pro-democracy, Kurdish and Islamic State fighters and interfering with the US-led coalition's operations in and around Syria (McLeary, 2018). The alleged use of cyber attacks and jamming of GPS signals during TRJE18 are further evidence of Russia's willingness to use offensive cyber and EW capabilities to disrupt NATO operations, with cascading effect across multiple domains (Tigner, 2018). Most recently, military exercises in the Central and Southern Military Districts as part of Kavaz 2020 have provided perhaps the most explicit public acknowledgement of Russia's ambition to implement its own variant on multi-domain concepts. One of 'the key features of the manoeuvres was to use [multi-domain] force groupings to commence and repel a 'global strike' from a simulated adversary' representing the US or NATO and to organise Russia's counter-action as a 'multi-sphere operation' (mnogosfernoy operatsii— seen by observers as "apparently the Russian General Staff's interpretation of the US term, 'multi-domain operations'") (McDermott, 2020).

These conceptual developments and real-world applications illustrate how Russian commanders increasingly use cyber-attacks to create windows of opportunity for success in the early stages of a conflict, while also enabling the execution of offensive tasks in other domains to achieve victory (Sprang, 2018).

2) People's Republic of China

China's strategic concepts are also increasingly characterised by joint and multi-domain thinking, the People's Liberation Army (PLA) understanding the future battlespace as an all-domain confrontation between networked, information-dependent systems-of-systems. Acknowledging increasing interdependencies within and between domains, the PLA aims to harness cyber capabilities to exploit seams and vulnerabilities within adversary networks. Chinese doctrine, therefore, centres on concepts of 'informatised warfare' and

[7] Including the battles of Zelenopillya (2014), Ilovaisk (2014), Donetsk Airport (2014-15), and Debal'tseve (2015). See: Sprang, 2018 and Griesemer, 2018.

multi-domain 'systems confrontation' designed to prepare for future conflict with a technologically advanced opponent (Engstrom, 2018; Kilcullen, 2020).

Parallels can be drawn with Western multi-domain thinking. 'Informatised warfare' recognises the growing information-dependency of military operations and seeks to acquire, transmit, process and use information to conduct cross-domain operations and seize tactical opportunities through an enhanced, shared awareness of the battlespace (DIA, 2019). 'Systems confrontation' or 'systems attack', known as China's 'basic operational method' of warfare, aims to defeat militarily superior opponents by exploiting vulnerabilities in their integrated, networked systems. This entails systematically targeting linkages and nodes that hold an advanced network-centric force together as a cohesive whole (US Joint Staff, 2018).

China is therefore seeking to use cyberspace and the EMS to disrupt and fracture the adversary's system-of-systems and achieve information and decision advantage over a paralysed, disoriented and demoralised US or NATO (Engstrom, 2018; Kilcullen, 2020). The PLA understands activities in cyberspace and the EMS as critical integrators and enablers of kinetic operations in physical domains and arenas for influence operations within informatised warfare (OSD, 2019). China's information warfare strategy, known as 'integrated network electronic warfare', entails the integrated use of cyber-attacks, electronic warfare (EW) and targeted kinetic strikes on critical nodes in command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) networks; this must be underpinned by a fully networked digital architecture to integrate PLA joint operations across domains (Scouras, Smyth & Mahnken, 2017).

China's efforts to implement this vision are evidenced through the PLA's recent force restructuring. In December 2015, it formed the Strategic Support Force (SSF), with the stated purpose of improving the PLA's capacity for operating in the cyber, electromagnetic and space domains (Kania & Costello, 2018). One of the SSF's primary roles is strategic information operations—the integration and coordination of cyber-espionage and offence, space and EW within a unified force to 'paralyse the enemy's operational system-of-systems' and 'sabotage the enemy's war command system-of-systems' in the initial stages of conflict (Costello & McReynolds, 2018: p. 2). China is similarly investing heavily in artificial intelligence (AI) to enable improved sensor and shooter integration, situational awareness and lethality, and more rapid and automated decision-making exploiting adversaries' OODA loops.[9] It seeks to move beyond 'informatised' to 'intelligentised' warfare in future (Bommakanti, 2020; Kania, 2020). Even in the context of sub-threshold operations, China's offensive cyber capabilities are being used both to compromise military and government networks directly and to target underlying supply chains and critical infrastructure (IISS, 2019).

[9] The OODA (observe-orient-decide-act) loop describes the iterative decision-making process of military commanders. See Zager & Zager, 2017.

Situated in a context of broader PLA restructuring, the SSF's establishment highlights China's efforts to operationalise cyberspace through increasingly integrated force structures capable of conducting operations across domains (Pollpeter et al., 2017; Costello & McReynolds, 2018). PLA modernisation remains an ongoing effort and its capabilities are not yet fully configured to deliver its stated strategy of 'systems attack' in a full-scale conflict (IHS Jane's, 2020). However, ongoing capability development and the recent overhaul of approaches to joint training and exercises indicate China is investing heavily in realising Xi Jinping's stated ambition of the PLA becoming a 'world-beating' all-domain force by 2049 (Cozad, 2016). Therefore, while China's systems-based, multi-domain understanding of cyberspace is currently reflected in doctrine and reform programmes, in the future it may be demonstrated through real-world operations (IHS Jane's, 2020).

3) Other Potential Adversaries

While their concepts and capabilities are less well-developed, smaller nations such as Iran and the DPRK are also investing heavily in cyberspace and exploring the effects on other domains. There is limited evidence of explicit multi-domain thinking within the current doctrine or activities of either country; however, both are seeking to enhance the use of cyber capabilities within their own joint operations. Iran's concepts of 'Retaliatory Deterrence' and 'Mosaic Warfare'[10] increasingly seek to exploit the cyber domain and encourage more deeply integrated joint operations, primarily aimed at deterring US-led intervention. Capitalising on opportunities presented by new technologies, Teheran is investing in cyber forces and capabilities to extend the reach of its deterrence strategy in conjunction with long-range ballistic and cruise missiles (McInnis, 2017; DIA, 2019). The DPRK is also pursuing an apparent shift towards warfighting beyond the traditional domains, viewing cross-domain integration and coordination of effects as a 'force multiplier' (Paul et al., 2018). This includes leveraging cyberspace and the EMS to defeat a militarily superior adversary by targeting vulnerabilities or dependencies within C2 networks to undermine cohesion within or between allied adversaries and erode their will to fight (Paul et al., 2018; Tasic, 2019).

3. IMPLICATIONS FOR NATO

Ongoing initiatives by Allies and adversaries alike emphasise the need to consider future threats in cyberspace and the EMS not in isolation but rather in terms of convergence with operations and vulnerabilities in other domains. At the Alliance level, these complex interlinkages present both opportunities and challenges for NATO. Novel technologies and concepts associated with cyberspace, space and information operations or activities in the EMS potentially offer new ways and means to understand, influence, deter and ultimately defeat adversaries through MDO. There are, however, considerable gaps between future ambitions and present realities. Addressing known shortfalls in cyber capabilities and MDO at the national level

[10] Not to be confused with the Defense Advanced Research Project Agency's emerging concept of Mosaic Warfare. See: Clark et al., 2020.

represents a significant, long-term and resource-intensive challenge. Integrating and cohering initiatives across an Alliance of 30 nations only increases the complexity of transformation 'exponentially' (Sharpy, 2020).

To address growing external threats posed by adversaries employing cyber-attacks as part of cross-domain manoeuvre, NATO must first understand its internal barriers, limitations and vulnerabilities regarding MDO. Only then can Allies agree a common approach to developing the future concepts, policies and permissions, C2, capabilities and innovation ecosystem required to compete in such a contested operational environment. The following sections address each of these themes in turn.

A. Conceptual Difficulties

NATO's challenges start with language (Heren, 2020; Reilly, 2020). There is no single definition of MDO employed consistently across the US services, let alone NATO (Donnelly & Farley, 2019; Smagh, 2020). According to Jeff Reilly of the US Air Command and Staff College, the ongoing revolution in the technology and threat environment 'mandates a greater investment of intellectual energy in the concept before it will be accepted by the military and defence communities within NATO' (Reilly, 2020: p. 2). This includes wargaming, modelling and simulation and experimentation to socialise, stress-test and refine MDO concepts (Zadalis, 2018).

Though arguably most mature in its thinking, the US is still working to build a common understanding of domains and of MDO, including why it is necessary, how it is novel or different from joint operations, and how to translate it into practice; including through a new Joint Warfighting Concept and related initiatives such as Joint All-Domain Command and Control (JADC2) capabilities (Grispen-Gelens, 2020). NATO remains even earlier in development: explicit MDO terminology such as convergence is largely absent from NATO doctrine, and has only recently begun featuring in national documents among European Allies such as France, Norway and the UK (Watling & Roper, 2019).

Whether 'multi-domain' is an enduring concept or simply the latest 'buzzword' in military thinking also remains to be seen. If the latter, there is a chance that US thinking may shift away from MDO before NATO has even begun to fully mature its own concept (Spirtas, 2018). As with many buzzwords, there is potential for conceptual confusion or for misappropriation of the latest fashionable concept to provide political and intellectual cover for enduring competition among individual service branches for new funding and responsibilities in emerging domains such as cyberspace and space (Grest & Heren, 2019).

NATO is evolving its understanding of multi-domain synergies while doctrine, policies, plans, C2 structures and capabilities for the cyber and space domains remain immature. The Allies approved a high-level Military Vision and Strategy on Cyberspace as a Domain of Operations in June 2018 (NATO, 2020b) and NATO only recently published the first edition of *AJP-*

3.20 Allied Joint Doctrine for Cyberspace Operations covering cyberspace operations in January 2020. Reservations lodged by Allies include US concerns about how NATO defines and understands domains and the information environment (NATO, 2020c). NATO is also busy operationalising the *Military Strategy* adopted in 2019, implementing readiness initiatives, developing theatre-wide strategies, and graduated response plans, and working up both the NWCC and a new *Concept for the Deterrence and Defence of the Euro-Atlantic Area* (NATO, 2019a; NATO, 2020f). With so many competing priorities already on the Alliance's agenda, finding the political, institutional and intellectual bandwidth needed to agree a common lexicon and concept of MDO—and cyberspace's role therein—is a challenge.

NATO faces another difficulty not shared by adversaries. While Russia and China can focus conceptual, force and capability development efforts on a specific foe (the US and NATO) and region (their near abroad), NATO must plan and prepare for wide-reaching scenarios. A multi-domain concept and set of forces configured to address Russia in northern and eastern Europe might be ill-suited to operating in the Mediterranean, countering Iran in the Gulf, or deterring China in the Indo-Pacific. One potential risk is a divergence between US efforts to design MDO and JADC2 networks primarily to address China and any NATO system-of-systems for MDO oriented towards Russia (Grispen-Gelens, 2020).

B. Policy Tensions

Policy differences exacerbate conceptual ones. Allies differ in their policy and legal constraints, strategic cultures, threat perception, resources, planning and budgetary cycles and forces (Sondhaus, 2006). While solidarity ultimately remains NATO's strongest asset, these differences create seams that adversaries can exploit. This is especially so with cyberspace, where there is more sensitivity and less commonality to emerging national approaches than in more established domains, and to MDO, which is inherently predicated on integration and interoperability (Sharpy, 2020).

Information sharing is especially problematic for the cyber dimension of MDO, with Allies reticent to share details of their capabilities across NATO given security concerns and political sensitivities. The issue of permissions is also a 'significant challenge in the development of cyber capabilities', especially where reconnaissance on Allied soil and networks is required to detect hostile cyber activity (Watling & Roper, 2019). Nations also have differing policy, legal and ethical stances on key technologies on which MDO relies. This includes the use of offensive cyber capabilities or basing of hypersonic missiles or long-range penetrating fires in Europe, which some fear could be destabilising and escalatory (Quintin & Vanholme, 2020). NATO similarly lacks a common approach to governance and use of AI, autonomy and automation, all envisaged as essential enablers for JADC2 (Williams, 2020). This affects the levels of autonomy (with the human in, on or out of the loop) used for sensor data fusion and decision-making, or to deliver effects using uncrewed platforms, automated cyber systems and human-machine teaming (Scharre, 2018).

In considering cooperation and burden-sharing, Allies face several dilemmas depending on their ambitions and resources for both cyberspace and MDO. The US must overcome domestic inter-service rivalries and decide how to integrate partners, including whether it can accept a multinational vision of MDO that is not imposed on smaller allies—or excludes them entirely, at NATO's expense—but rather is genuinely collaborative (Watling & Roper, 2019). Larger European nations face the dilemma of whether to buy into a US-led architecture and system-of-systems with implications for freedom of action, data-sharing and procurement choices, or shoulder the costs of sovereign or multinational alternatives.[11] They also face choices over how best to contribute to multinational MDO: whether to aspire to full-spectrum capabilities to allow sovereign action and offer redundancy to Allies' capabilities or to specialise in certain domains (e.g. cyber) to offer niche capability and buy leverage with the US and NATO by making themselves indispensable. Smaller nations must decide how to influence larger Allies and NATO, and what to do if they lack cyber capabilities (or others deemed central to MDO, e.g. long-range fires) or their forces are too small to operate or gain MDO experience at echelons above brigade (Watling & Roper, 2019).

The economic fallout of COVID-19 also raises renewed questions about affordability and the extent to which Allies are willing and able to invest in new cyber capabilities—though some may see these as cost-efficient alternatives to land, air or maritime forces—and how they time investments in ambitious transformation programmes such as MDO (Clark, 2020). Timing presents both threats and opportunities from a cyber perspective. Rapid, hasty transformation risks undermining NATO cohesion and interoperability or creating vulnerabilities in JADC2 systems with immature cyber defences (Donaldson & Sciarini, 2019b). Conversely, overly cautious change risks ceding ground to adversaries such as Russia and China which are investing heavily in asymmetric means, including offensive cyber capabilities, to gain an information advantage over NATO (Kilcullen, 2020).

The most likely outcome may be a variegated approach, with some Allies (including the US) taking the lead on conceptual and capability development for MDO, creating national or mini-lateral networks for JADC2, and then building up a looser degree of interoperability at NATO level (Watling & Roper, 2019).

C. Capability and Force Development Priorities

Assuming NATO can overcome conceptual and policy hurdles, significant effort will still be required to develop the necessary forces and capabilities across all domains, but perhaps especially for cyberspace.

Operationalising MDO demands a 'calibrated force posture' with multi-domain formations strategically positioned, held at readiness and able to de-

[11] E.g. development of a 'combat cloud' within the Franco-German Future Combat Air System. See: Airbus, 2020.

ploy over large distances, trained and equipped to operate across multiple contested domains (Grispen-Gelens, 2020). The vision is for different sensors and shooters to share and fuse data, build a common operating picture, inform rapid decision-making and deliver effects at a time and place of the commander's choosing and to do so agnostic of domains, nation, service or platform (Niewood, Grant & Lewis, 2019). Forces must operate at pace and against an adversary contesting all domains. This tempo necessitates moving beyond NATO's past focus on synchronisation of pre-planned effects in individual domains towards more agile targeting and more resilience against hostile attempts at 'disorganisation' or 'systems attack' (Thomas, 2019; Engstrom, 2018).

Linking all this together demands novel approaches to C4ISR, as reflected in investments in JADC2 (Harrigian, 2020). This US initiative leverages advances in information and communication technologies such as mesh networks, cloud and edge computing, open architectures, data analytics, AI and machine learning, autonomy and automation, software-defined systems, robotics, satellite communications and sophisticated cyber and EMS capabilities (Hitchens, 2019). Future JADC2 networks must be secure, robust, resilient, agile and more decentralised, with enough bandwidth to share data in a timely and secure manner despite cyber attacks, jamming, spoofing or physical destruction of communication nodes (Goldfein, 2017). Trust is also essential, handling data from different sources and at multiple security levels without making controls so arduous that users and devices cannot access the network (Donaldson & Sciarini, 2019a).

Reliance on connectivity makes cyberspace, space and the EMS the 'centre of gravity' for MDO (Hess et al., 2019). JADC2 introduces obvious challenges from a cyber threat perspective, both in terms of the attack surface for different threat vectors and the cascading effects from hostile cyber activity—though, of course, existing centralised C2 hubs also have their own vulnerabilities to cyber or physical attack (Hess et al., 2019). Improved cyber capabilities are not only needed to secure and enable operations in other domains (Reilly, 2020). Investments by Russia and China to contest cyberspace and the EMS may also limit the ability of NATO commanders to employ offensive cyber capabilities at a time and place that will 'converge' with effects through other domains. Securing networks against disruption is critical at the operational and strategic levels given requirements for reach-back to headquarters, especially constraining organisations responsible for delivering offensive cyber effects, since these are likely to be physically located in the homeland (Watling & Roper, 2019; Nettis, 2020).

D. Challenges for Command and Control

Any shift towards MDO also raises difficult questions about C2. NATO is arguably already challenged by seams when executing joint warfare, let alone a more ambitious vision of future JADC2 (Perkins & Olivieri, 2018; Zadalis, 2018). In broad terms, this could adopt a more hierarchical or de-centralised model, each with associated benefits, costs and risks (DCDC, 2015). The

NATO C2COE has launched an MDO C2 demonstrator to explore these issues, including how new technology might enable accelerated decision-making, reduced reliance on siloed physical command centres and a re-imagining of mission command for future MDO (NATO C2COE, 2020a).

Problematically, authorities associated with using cyber capabilities are typically held at the strategic and national level; how tactical or operational commanders might call upon cyber means as part of future MDO remains unclear (Nettis, 2020). Responsibilities for cyberspace also often fall at least partly to civilian agencies, adding the complexity of cross-government co-operation. The private sector's role developing and applying technologies in the cyber domain (and, increasingly, space) also necessitates that NATO work more closely with industry, academia and others than for land, maritime or air operations (Ablon et al., 2019). This presents operational, policy and legal difficulties for C2, and cybersecurity challenges associated with reliance on industry-owned networks, though Allies continue to evolve novel mechanisms for partnering with industry to address cyber threats (Carr, 2016).

There is also the question of tempo: how to synchronise operations in cyberspace with the delivery of effects in other domains (Reilly, 2020). Though cyber attacks might initiate in a moment, the underlying tools and exploits may take years to develop and the lead times and scale of their eventual effect may be difficult to predict or measure given the difficulties with battle damage assessment in cyberspace or the EMS (Patrikarakos, 2017; US Joint Staff, 2019). Similarly, commanders may lack awareness or understanding of available cyber instruments and their limitations and effects compared to more familiar weapons in the physical domains, limiting inclusion in joint planning and decision-making (Carbonell, 2017).

E. Innovation and Transformation

Finally, NATO also faces vulnerabilities and risks associated with the pace of tactical and technological innovation in both the cyber domain and MDO. These change not only the capabilities that NATO requires, but also how it develops, acquires, trains, fields, exercises and sustains them, necessitating transformation across all components of the DOTMLPF-I framework and all stages of the capability lifecycle.[12]

Developing new technology is necessary but insufficient to deliver the cyber, C4ISR and other capabilities needed to realise ambitions for MDO (Dwyer, 2020). Technical standards and a broader enterprise architecture approach to manage and coordinate are essential. Yet despite increasing automation, the human dimension also remains key (Carbonell, 2017). There are several unanswered questions to consider, answers to which will shape whether NATO or its adversaries gain advantage in cyberspace and future MDO: how to deliver multi-domain education, training and exercising, including

[12] Doctrine, organisation, training, materiel, leadership, personnel, facilities and interoperability (DOTMLPF-I) is the mnemonic aid used by NATO military planners to consider the issues and perspectives required to field a new capability.

through challenging scenarios that allow learning through failure and make cyberspace a key consideration for non-cyber audiences (Perkins & Olivieri, 2018); how to bring together disparate modelling and simulation initiatives, integrating synthetic environments for individual domains into a single integrated architecture[13] allowing realistic simulations of MDO and the cross-domain effects of cyber, electronic and information warfare (McArdle, 2019); how to build a multi-domain culture and mindset that overcomes traditional stovepipes, such as territoriality by individual services or command structures (Goldfein, 2017; Heren, 2020); and how to maintain a pipeline of relevant skills and expertise, both for cyber defence and multi-domain integration, and offer career paths for specialists (Ablon et al., 2019).

Ensuring NATO is resilient against fast-changing cyber and multi-domain threats also requires enhancing its agility and adaptability (Ozdemir, 2020). This includes reforming capability development processes to reduce lead times—especially important for cyber capabilities—and increasing organisations' capacity to identify disruptive innovations and absorb them at pace (Ablon et al., 2019). This necessitates models such as agile and spiral development or DevSecOps, genuine partnerships with industry and academia and increased end-user involvement in systems design (Harrigian, 2020; Sharpy, 2020). Realising such transformation requires changes across DOTMPLF-I, including strong and sustained leadership, appropriate and coordinated investment of resources and a different attitude towards risk in areas such as acquisition, training and experimentation to operationalise cyberspace as part of MDO (Niewood, Grant & Lewis, 2019).

ACT, the NATO Communications and Information Agency and individual Allies are already taking steps to address barriers to agile capability development and innovation. However, there remains more to do and change takes time (Grand & Gillis, 2020). Lessons learned from past programmes offer insights into what enables success, but also urge realism about how difficult and long a process it can be to implement reforms in complex military bureaucracies and multinational settings (Sharpy, 2020). Examples cited include the case of AirLand Battle, which for all its ambition could not eradicate the deep-seated differences between the US Army and US Air Force cultures and views on warfighting (Johnson, 2018); the development and promulgation of Link 16 across the Alliance, which has taken almost half a century to overcome both technical and cultural barriers to interoperability (Hura et al., 2000); or NATO's hard-fought efforts to enhance chemical, biological, radiological and nuclear capabilities since the 1990s (Ablon et al., 2019). Tellingly, militaries are still working to better integrate land, sea and airpower, suggesting it may take decades to fully understand the complex synergies with cyberspace, the EMS and space (Reilly, 2020).

[13] For example, UK Strategic Command has partnered with technology company Improbable to explore the feasibility of high-fidelity modelling and simulation of multi-domain operations through its Single Synthetic Environment (SSE) Technology Demonstrator, with the British Army also contracting Improbable to help develop its SSE roadmap. See Improbable, 2020.

4. CONCLUSION

In conclusion, cyber threats do not exist in a vacuum, nor are NATO's cyber operations divorced from developments on land, at sea, in the air or in space. According to emerging concepts in the US and other Allied nations, the future is 'multi, multi, multi' (Schanz, 2014: p. 40). This necessitates thinking beyond existing conceptual or institutional boundaries and understanding cyber developments in their wider context: multi-domain, multi-sensor, multi-shooter, multi-mission, multi-service and multi-national. This requires education, training and cultural reform to instil multi-domain thinking at all levels: from junior military personnel and international civilian staff up to the most senior political-military leaders.

Such thinking avoids the pitfalls of oversimplified analysis but, equally, brings the challenge of complexity. Fortunately, NATO is one of the great success stories of an organisation harmonising different perspectives, institutions, cultures, capabilities and effects in pursuit of a common goal; the Alliance is already a system-of-systems of a kind (Sharpy, 2020). However, it faces complex and fast-changing challenges as it evolves from an analogue to a digital alliance and begins to embrace cyberspace and MDO. These stem both from external adversaries such as the evolving theory and practice of disorganisation and reflexive control by Russia or systems attack by China, and internal barriers to NATO cohesion. Continuing to improve understanding of the interlinkages between these different threats and risks is essential to inform the transformation process needed to realise NATO's ambitions for the cyber domain and for multi-domain more broadly.

5. REFERENCES

Ablon, L., Binnendijk, A., Hodgson, Q., Lilly, B., Romanosky, S., Senty, D., & Thompson, J. (2008) *Operationalizing Cyberspace as a Military Domain: Lessons for NATO.* Santa Monica, CA: RAND Corporation, PE-329-NATO. [Accessed 13th August 2020]. Available from: https://www.rand.org/pubs/perspectives/PE329.html.

Adamsky, D. (2015) *Cross-Domain Coercion: The Current Russian Art of Strategy.* Proliferation Papers 54, Institut Français des Relations Internationales (Ifri). Available from: https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf [Accessed 12th August 2020].

Airbus. (2020) *Airbus and Thales Join Forces to Develop the Air Combat Could for Future Combat Air System*. Airbus, 19 February 2020. Available from: https://www.airbus.com/newsroom/news/en/2020/02/airbus-and-thales-join-forces-to-develop-the-air-combat-cloud-for-future-combat-air-system.html [Accessed 22nd September 2020].

Asian Military Review. (2020) *China Broadens Cyber Options*. Asian Military Review, 15 January 2020. Available from: https://asianmilitaryreview.com/2020/01/china-broadens-cyber-options/ [Accessed 24th September 2020].

Barry, B. (2020) *New UK Strategic Command Faces Early Challenges*. IISS Military Balance [online]. 19 June 2020. London: International Institute of Strategic Studies. Available from: https://www.iiss.org/blogs/military-balance/2020/06/uk-strategic-command-challenges-covid-19 [Accessed 13th August 2020].
Bommakanti, K. (2020) *AI in the Chinese Military: Current Initiatives and the Implications for India.* Occasional Paper [online], Observer Research Foundation. February 2020. Available from: https://www.orfonline.org/research/a-i-in-the-chinese-military-current-initiatives-and-the-implications-for-india-61253/ [Accessed 14th August 2020].
Brent, L. (2019) *NATO's Role in Cyberspace*. NATO Review [online]. 12 February 2019. Available from: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html [Accessed 11th August 2020].
Brzozowski, A. (2018) *NATO Sees New Cyber Command Centre by 2023 as Europe Readies for Cyber Threats.* Euractiv [online]. 17 October 2018. Available from: https://www.euractiv.com/section/defence-and-security/news/nato-sees-new-cyber-command-centre-by-2023-as-europe-readies-for-cyber-threats/ [Accessed 22nd October 2020].
Carbonell, J. (2017) *Getting off the Bench: Challenges to Integrating Cyber into Multi-Domain Operations.* OTH: Multi-Domain Operations & Strategy [online]. 1 June 2017. Available from: https://othjournal.com/2017/06/01/cyber-challenges-mdo/ [Accessed 12th August 2020].
Carr, M. (2016) Public-Private Partnerships in National Cyber-Security Strategies. *International Affairs.* 92 (1), 43-62. Available from: https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf [Accessed 13th August 2020].
Carter, N. (2019) *New UK Strategic Command to Drive Integration for Multi-Domain Effect*. SC Magazine UK 5 December 2019. Available from: https://www.scmagazineuk.com/new-uk-strategic-command-drive-integration-multi-domain-effect/article/1667949 [Accessed 11th August 2020].
Clare, P. (2020) *The Answer is Multi-Domain Operations – Now What's the Question?* Wavell Room. 13 February 2020. Available from: https://wavellroom.com/2020/02/13/the-answer-is-multi-domain-operations-now-whats-the-question/ [Accessed 7th August 2020].
Clark, B. (2020) *JADC2 and AI Should Enable Post-Pandemic Military Creativity, Not Replace It.* Hudson Institute. 9 May 2020. Available from: https://www.hudson.org/research/16019-jadc2-and-ai-should-enable-post-pandemic-military-creativity-not-replace-it [Accessed 13th August 2020].
Clark, B., Patt, D., & Schramm, H. (2020) *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations.* Center for Strategic and Budgetary Assessments (CSBA), 11 February. Available from: https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations [Accessed 20th September 2020].
Conti, G. & Raymond, D. (2017) *On Cyber: Towards an Operational Art for Cyber Conflict.* Kopidion Press.
Conti, G. & Fanelli, R. (2019) 'How could they not: thinking like a state cyber threat actor'. *The Cyber Defense Review*. (4) 2, 49-64. Available from: https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/CDR%20V4N2-Fall%202019.pdf [Accessed 22nd September 2020].
Costello, J. & McReynolds, J. (2018) China's Strategic Support Force: A Force for a New Era. *China Strategic Perspectives 13* [online]. Institute for National Strategic Studies (INSS), National Defense University. Available from: https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-per-

spectives_13.pdf [Accessed 8th August 2020].
Cozad, M. (2016) *PLA Joint Training and Implications for Future Expeditionary Operations*. Santa Monica, CA: RAND Corporation, CT-451. Available from: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT451/RAND_CT451.pdf [Accessed 12th August 2020].
Development, Concepts and Doctrine Centre (DCDC). (2015) *Future Operating Environment 2035*. Strategic Trends Programme. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/646821/20151203-FOE_35_final_v29_web.pdf [Accessed 9th August 2020].
Development, Concepts and Doctrine Centre (DCDC). (2017) *Joint Concept Note 2/17 Future of Command and Control.* Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643245/concepts_uk_future_c2_jcn_2_17.pdf [Accessed 11th August 2020].
Defense Acquisition University (DAU). (2020) Chapter 3: Systems Engineering. In: *US Defense Acquisition Guidebook.* Fort Belvoir, VA: USA. Available from: https://www.dau.edu/guidebooks/_layouts/15/WopiFrame.aspx?sourcedoc=/guidebooks/Shared%20Documents/Chapter%203%20Systems%20Engineering.pdf&action=default [Accessed 8th August 2020].
Defense Intelligence Agency (DIA). (2019) *China Military Power: Modernizing a Force to Fight and Win.* DIA-02-1706-065. Available from: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf [Accessed 11th August 2020].
Donaldson, J. & Sciarini, C. (2019a) *Vulnerabilities of Multi-Domain Command and Control (Part 1)*. OTH: Multi-Domain Operations & Strategy. 4 March 2019. Available from: https://othjournal.com/2019/03/04/vulnerabilities-of-multi-domain-command-and-control-part-1/ [Accessed 11th August 2020].
Donaldson, J. & Sciarini, C. (2019b) *Vulnerabilities of Multi-Domain Command and Control (Part 2)*. OTH: Multi-Domain Operations & Strategy. 6 March 2019. Available from: https://othjournal.com/2019/03/06/vulnerabilities-of-multi-domain-command-and-control-part-2/ [Accessed 11th August 2020].
Donnelly, J. & Farley, J. (2019) *Defining the 'Domain' in Multi-Domain*, in the Joint Air Power Competence Centre, Joint Air and Space Power Conference 2019: Shaping NATO for Multi-Domain Operations of the Future (2019): 7-11. Available from: https://www.japcc.org/defining-the-domain-in-multi-domain/ [Accessed 20th September 2020].
Dwyer, M. (2020) *Making the Most of the Air Force's Investment in Joint All Domain Command and Control*. Center for Strategic & International Studies (CSIS). 6 March 2020. Available from: https://www.csis.org/analysis/making-most-air-forces-investment-joint-all-domain-command-and-control [Accessed 11th August 2020].
Engstrom, J. (2018) *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare.* Santa Monica, CA: RAND Corporation, RR-1708-OSD. Available from: https://www.rand.org/pubs/research_reports/RR1708.html [Accessed 10th August 2020].
Feickert, A. (2020) *Defense Primer: Army Multi-Domain Operations (MDO)*. Briefing prepared by the Congressional Research Service. 19 January 2020. Available from: https://fas.org/sgp/crs/natsec/IF11409.pdf [Accessed 9th August 2020].
Freedberg, S. (2018) *Army Multi-Domain Update: New HQs, Grey Zones & The Art of the Unfeasible*. Breaking Defense. 7 December 2018. Available from: https://breakingdefense.com/2018/12/army-multi-domain-update-new-hqs-grey-zones-the-art-of-the-unfeasible/ [Accessed 13th August 2020].

Galeotti, M. (2016) 'Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?' *Small Wars and Insurgencies*. 27 (2). 21 March 2016. Available from: https://www.tandfonline.com/doi/abs/10.1080/09592318.2015.1129170 [Accessed 11th August 2020].
Goldfein, D. (2017) *Enhancing Multi-Domain Command and Control… Tying it All Together.* Washington, DC: United States Air Force. Available from: https://www.af.mil/Portals/1/documents/csaf/letter3/Enhancing_Multi-domain_CommandControl.pdf [Accessed 13th August 2020].
Grand, C. & Gillis, M. (2020) Alliance Capabilities at 70: Achieving Agility for an Uncertain Future. *NDC Policy Brief* No.1 January 2020. Available from: http://www.ndc.nato.int/download/downloads.php?icode=622 [Accessed 14th August 2020].
Grest, H. & Heren, H. (2019) *What is a Multi-Domain Operation?* in the Joint Air Power Competence Centre, Joint Air and Space Power Conference 2019: Shaping NATO for Multi-Domain Operations of the Future (2019): 1-3. Available from: https://www.japcc.org/what-is-a-multi-domain-operation/ [Accessed 20th September 2020].
Griesemer, T. (2018) *'Russian Military Reorganization: A Step Towards Multi-Domain Operations'.* OTH: Multi-Domain Operations & Strategy, 11 November 2018. Available from: https://othjournal.com/2018/11/19/russian-military-reorganization-a-step-toward-multi-domain-operations/ [Accessed 11th August 2020].
Grispen-Gelens, C. (2020) *Cohesion Through Convergence?* Seminar MDO Read Ahead, NATO C2COE, 1 July 2020. Available from: http://c2coe.org/download/seminar-2020-read-ahead-carlina-grispen-gelens-cohesion-through-convergence/ [Accessed 11th August 2020].
Harrigian, Jeffrey L. (2020) Shaping the Future Multi-Domain C2. *Joint Air Power Competence Centre (JAPCC) Journal.* 29 (1). Available from: https://www.japcc.org/shaping-the-future-multi-domain-c2/ [Accessed 12th August 2020].
Heren, H. (2020) 'Multi-Domain Operations: Inconceivable!'. *Joint Air Power Competence Centre (JAPCC) Journal.* 29 (1). Available from: https://www.japcc.org/multi-domain-operations-inconceivable/ [Accessed 12th August 2020].
Hess, J, Kiser, A., Bouhafa, E.M., & Williams, S. (2019) *The Combat Cloud: Enabling Multidomain Command and Control across the Range of Military Operations.* Wright Flying Papers, Air Command and Staff College. February 2019. Available from: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/wf_0065_hess_combat_cloud.pdf [Accessed 14th August 2020].
Hitchens, T. (2019a) *Multi Domain drive NATO Industry to Craft New Air Power Interoperability.* Breaking Defense. 15 November 2019. Available from: https://breakingdefense.com/2019/11/multi-domain-drives-nato-industry-to-craft-new-air-power-interoperability/ [Accessed 12th August 2020].
Hitchens, T. (2019b). *OSD, Services Get First Look at Air Force Multi-Domain Chops.* Breaking Defense, 23 December 2019. Available from: https://breakingdefense.com/2019/12/osd-services-get-first-look-at-air-force-multi-domain-chops/ [Accessed 14th August 2020].
Hura, M., McLeod, G., Larson, E., Schneider, J., Gonzales, D., Norton, D., Jacobs, J., O'Connell, K., Little, W., Mesic, R., & Jamison, L. (2000) *Interoperability: A Continuing Challenge in Coalition Air Operations.* Santa Monica, CA: RAND Corporation, MR-1235-AF. Available from: https://www.rand.org/pubs/monograph_reports/MR1235.html [Accessed 21st September 2020].
IHS Jane's. (2020) *China – Defence Budget Overview.* Jane's Sentinel Security Assessment – China and Northeast Asia. 22 January 2020. Available from: https://janes.ihs.com/Janes/Display/chins090-cna [Accessed 9th August 2020].

Improbable. (2020) *Improbable Secures Pathfinder Technology Demonstrator Contract with British Army.* 6 August. Available from: https://improbable.io/blog/uk-army-cttp-sse [Accessed 13th August 2020].
International Institute for Strategic Studies (IISS). (2019) 'China's Cyber Power in a New Era' in *Asia Pacific Regional Security Assessment* 2019, IISS, May 2019. Available from: https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5 [Accessed 24th September 2020].
Johnson, D. (2018) *Shared Problems: The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle.* Santa Monica, CA: RAND Corporation. PE-301-A/AF. Available from: https://www.rand.org/pubs/perspectives/PE301.html [Accessed 13th August 2020].
Joiner, K. & Tutty, M. (2018) 'A tale of two allied defence departments: new assurance initiatives for managing increasing system complexity, interconnectedness and vulnerability'. *Australian Journal of Multi-Disciplinary Engineering.* 14 (1). Available from: https://www.tandfonline.com/doi/full/10.1080/14488388.2018.1426407?casa_token=NQjkdhyasGUAAAAA%3AqkxJ_XQlQSkacMHo_TE13gLRUFzB7ANaj42zxuUeGRuun3WOYYC0ALeNRdui_BPgiuV8Rbpq31Y [Accessed 22nd September 2020].
Kania, E. & Costello, J. (2017) *China's Quest for Informatization Drives PLA Reforms.* The Diplomat, 4 March 2017. Available from: https://thediplomat.com/2017/03/chinas-quest-for-informatization-drives-pla-reforms/ [Accessed 10th August 2020].
Kania, E. (2020) *'AI Weapons' in China's Military Innovation.* The Brookings Institution in partnership with the Center for Security and Emerging Technology, April 2020. Available from: https://www.brookings.edu/research/ai-weapons-in-chinas-military-innovation/ [Accessed 14th August 2020].
Kilcullen, D. (2020) *The Dragons and the Snakes: How the Rest Learned to Fight the West.* Glasgow, UK: Bell & Bain Ltd.
Knighton, R. (2019) *Lord Trenchard Memorial Lecture 2019*. Royal United Services Institute (RUSI). November 18. Available from: https://rusi.org/event/lord-trenchard-memorial-lecture-2019 [Accessed 11th August 2020].
Lindsay, J. & Gartzke, E. (2020) Politics By Many Other Means: The Comparative Strategic Advantages of Operational Domains. *Journal of Strategic Studies*. Available from: https://doi.org/10.1080/01402390.2020.1768372 [Accessed 13th August 2020].
Manea, O. (2018) The Role of Offset Strategies in Restoring Conventional Deterrence. *Small Wars Journal*. Available from: https://smallwarsjournal.com/jrnl/art/role-offset-strategies-restoring-conventional-deterrence [Accessed 21st September 2020].
McArdle, J. (2019) *Victory Over and Across Domains: Training for Tomorrow's Battlefields.* Center for Strategic and Budgetary Assessments (CSBA), 25 January. Available from: https://csbaonline.org/research/publications/victory-over-and-across-domains-training-for-tomorrows-battlefields [Accessed 21st September 2020].
McDermott, R. (2020) Russian Armed Forces Test Multi-Domain Operations. *Eurasia Daily Monitor* [online]. 17 (123). Available from: https://jamestown.org/program/russian-armed-forces-test-multi-domain-operations/ [Accessed 21st September 2020].
McInnis, J. (2017) *Iranian Concepts of Warfare: Understanding Teheran's Evolving Military Doctrines*. American Enterprise Institute. February 2017. Available from: https://www.aei.org/research-products/report/iranian-concepts-of-warfare-understanding-tehrans-evolving-military-doctrines/ [Accessed 13th August 2020].

McLeary, P. (2018) 'Russia Winning Info & Electronic War in Syria, US & UK Generals Warn'. *Breaking Defense* [online], 9 October. Available from: https://breakingdefense.com/2018/10/russia-winning-information-electronic-war-over-syria-us-uk-generals-warn/ [Accessed 20th September 2020].
Nakasone, P. & Lewis, C. (2017) Cyberspace in Multi-Domain Battle. *The Cyber Defense Review* [online]. 2 (1), 15-26. Available from: https://www.jstor.org/stable/10.2307/26267397 [Accessed 11th August 2020].
Nettis, K. (2020) *Multi-Domain Operations: Bridging the Gaps for Dominance*. Sixteenth Air Force. 16 March 2020. Available from: https://www.16af.af.mil/News/Article/2112873/multi-domain-operations-bridging-the-gaps-for-dominance/ [Accessed 13th August 2020].
Niewood, E., Grant, G., & Lewis, T. (2019) *A New Battle Command Architecture for Multi-Domain Operations: Countering Peer Adversary Power Projection.* The MITRE Center for Technology & National Security, December 2019. Available from: https://www.mitre.org/sites/default/files/publications/Joint-All-Domain-Command-Control.pdf [Accessed 13th August 2020].
North Atlantic Treaty Organisation (NATO). (2018a). *Brussels Summit Declaration*. 11 July 2020. Available from: https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=uk [Accessed 23rd October 2020].
North Atlantic Treaty Organisation (NATO). (2018b). *Framework for Future Alliance Operations: 2018 Report*. Available from: https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf [Accessed 23rd October 2020].
North Atlantic Treaty Organisation (NATO). (2019a) *NATO: Ready for the Future. Adapting the Alliance (2018-2019).* 29 November 2019. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_191129-adaptation_2018_2019_en.pdf [Accessed 12th August 2020].
North Atlantic Treaty Organisation (NATO). (2019b) *AJP-3 Allied Joint Doctrine for the Conduct of Operations*, Edition C Version 1, February 2019. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf [Accessed 24th September 2020].
North Atlantic Treaty Organisation (NATO). (2020a) *NATO's approach to space*. Available from: https://www.nato.int/cps/en/natohq/topics_175419.htm [Accessed 13th August 2020].
North Atlantic Treaty Organisation (NATO). (2020b) *Cyber defence*. Available from: https://www.nato.int/cps/en/natohq/topics_78170.htm [Accessed 13th August 2020].
North Atlantic Treaty Organisation (NATO). (2020c) *Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operation*. London: Ministry of Defence. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf [Accessed 11th August 2020].
North Atlantic Treaty Organisation (NATO). (2020d) *NATO Warfighting Capstone Concept Experiment Workshop.* Available from: https://www.act.nato.int/articles/nato-warfighting-capstone-concept-experiment-workshop [Accessed 22nd October 2020].
North Atlantic Treaty Organisation (NATO). (2020e) *Military Committee Visits Joint Warfare Centre; NATO Military Leaders Discuss Warfare Development.* Available from: https://www.act.nato.int/articles/mc-visits-jwc-discuss-warfare-development [Accessed 22nd October 2020].
North Atlantic Treaty Organisation (NATO). (2020f) *NATO Chiefs of Defence Assess Current Adaptation and Future Requirements.* Available from: https://www.nato.int/cps/en/natohq/news_172672.htm [Accessed 22nd October 2020].

NATO Command and Control Centre of Excellence (NATO C2COE). (2020a) *Multi-Domain Operations C2 Demonstrator, a collaboration between NATO C2COE and civil partners.* 16 April 2020. Available from: https://c2coe.org/2020/04/16/multi-domain-operations-c2-demonstrator-a-collaboration-between-nato-c2coe-and-civil-partners/ [Accessed 8th August 2020].
NATO Command and Control Centre of Excellence (NATO C2COE). (2020b) *Multi-Domain Operations: "Keys to Master Complexity"*. Available from: https://c2coe.org/seminar/ [Accessed 12th August 2020].
NATO Science and Technology Organisation (STO). (2018) *Agile Multi-Domain C2 of Socio-Technical Enterprises in Hybrid Operations*. Available from: https://www.sto.nato.int/SitePages/newsitem.aspx?ID=3578&IsDlg=1 [Accessed 22nd October 2020].
NATO Science and Technology Organisation (STO). (2020) *Wargaming Multi-Domain Operations in an A2/AD Environment.* Available from: https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16876 [Accessed 22nd October 2020].
Office of the Secretary of Defense (OSD). (2019) *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019.* Available from: https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf [Accessed 13 August 2020].
Ozdemir, H. (2020) *Multi-Domain Operations from System Dynamics Perspective.* Seminar MDO Read Ahead, NATO C2COE. 10 July 2020. Available from: http://c2coe.org/download/seminar-2020-read-ahead-dr-hilmi-ozdemir-multi-domain-operations-from-system-dynamics-perspective/ [Accessed 11th August 2020].
Paul, C., Clarke, C., Schwille, M., Hlavka, J., Brown, M., Davenport, S., Porsche III, I., & Harding, J. (2018) *Lessons from Others for Future US Army Operations in and through the Information Environment: Case Studies*. Santa Monica, CA: RAND Corporation. RR-1925/2-A. Available from: https://www.rand.org/pubs/research_reports/RR1925z2.html [Accessed 10th August 2020].
Perkins, W. & Olivieri, A. (2018) On Multi-Domain Operations. *Joint Air Power Competence Centre (JAPCC) Journal.* 26 (1). Available from: https://www.japcc.org/on-multi-domain-operations/ [Accessed 12th August 2020].
Pollpeter, K, Chase, M., & Heginbotham, E. (2017) *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations.* Santa Monica, CA: RAND Corporation, RR-2058-AF. Available from: https://www.rand.org/pubs/research_reports/RR2058.html [Accessed 21st September 2020].
Quintin, A. & Vanholme, R. (2020) *Hypersonic Missiles and European Security: Challenges Ahead.* European Army Interoperability Centre (Finabel). 28 July 2020. Available from: https://finabel.org/hypersonic-missiles-and-european-security/ [Accessed 13th August 2020].
Reilly, J. (2020) *Creating Competitive Space Through a Framework of Joint All Domain Maneuver*. Seminar MDO Read Ahead, NATO C2COE. 23 July 2020. Available from: http://c2coe.org/download/seminar-2020-read-ahead-dr-jeff-reilly-creating-competitive-space-through-a-framework-of-joint-all-domain-maneuver/ [Accessed 12th August 2020].
Schanz, M. (2014) *The Combat Cloud.* Air Force Magazine, July 2014. Available from: http://www.airforcemag.com/MagazineArchive/Magazine%20Documents/2014/July%202014/0714combatcloud.pdf [Accessed 12th August 2020].
Scharre, P. (2018) *Army of None: Autonomous Weapons and the Future of War.* London, UK: W.W. Norton & Company.
Schneider, J. (2019) The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war. *Journal of Strategic Studies*. 42 (6), 841-863. Available from: https://www.tandfonline.com/

doi/abs/10.1080/01402390.2019.1627209 [Accessed 20th September 2020].
Scouras, J., Smyth, E., & Mahnken, T. (2017) *Cross-Domain Deterrence in US-China Strategy: Workshop Proceedings.* The John Hopkins University Applied Physics Laboratory. Originally published in 2014 and re-issued in 2017. Available from: https://www.jhuapl.edu/Content/documents/CrossDomainWeb.pdf [Accessed 11th August 2020].
Sharpy, T. (2020) *Multi-Domain Operations: The Future of Warfare.* Seminar MDO Read Ahead, NATO C2COE. 16 July 2020. Available from: http://c2coe.org/download/seminar-2020-read-ahead-lieutenant-general-sharpy-multi-domain-operations-the-future-of-warfare/ [Accessed 12th August 2020].
Shea, J. (2018) Cyberspace as a Domain of Operations: What is NATO's Vision and Strategy? *MCU Journal*. 9 (2), 133-150. Available from: https://doi.org/10.21140/mcuj.2018090208 [Accessed 10th August 2020].
Siegemund, M. (2018) *NATO Planning and Multi Domain Operations: A German Perspective.* OTH: Multi-Domain Operations & Strategy. 27 June 2018. Available from: https://othjournal.com/2018/06/27/nato-planning-and-multi-domain-operations-a-german-perspective/ [Accessed 9th August 2020].
Smagh, N. (2020) *Defense Capabilities: Joint All Domain Command and Control.* Briefing prepared by the Congressional Research Service. 6 April 2020. Available from: https://fas.org/sgp/crs/natsec/IF11493.pdf [Accessed 12th August 2020].
Sondhaus, L. (2006) *Strategic Culture and Ways of War.* Routledge Military Studies, Routledge.
Spirtas, M. (2018) *Towards one understanding of multiple domains.* RAND Corporation, 2 May 2018. Available from: https://www.rand.org/blog/2018/05/toward-one-understanding-of-multiple-domains.html [Accessed 24th September 2020].
Sprang, R. (2018) *Russia in Ukraine 2013-2016: The Application of New Type Warfare Maximizing the Exploitation of Cyber, IO and Media.* Small Wars Journal 11 September 2018. Available from: https://smallwarsjournal.com/jrnl/art/russia-ukraine-2013-2016-application-new-type-warfare-maximizing-exploitation-cyber-io-and [Accessed 9th August 2020].
Tasic, M. (2019). Exploring North Korea's Asymmetric Military Strategy. *Naval War College Review* [online]. 72 (4), 53-72. Available from: https://www.jstor.org/stable/10.2307/26775519 [Accessed 13th August 2020].
Thomas, T. (2019) *Russian Military Thought: Concepts and Elements.* MITRE Corporation. August 2019. Available from: https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf [Accessed 13th August 2020].
Tigner, B. (2018) *Electronic jamming between Russia and NATO is par for the course in the future, but it has its risky limits.* Atlantic Council, 15 November 2018. Available from: https://www.atlanticcouncil.org/blogs/new-atlanticist/electronic-jamming-between-russia-and-nato-is-par-for-the-course-in-the-future-but-it-has-its-risky-limits/ [Accessed 22nd September 2020].
Training and Doctrine Command (TRADOC). (2017) *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century* Version 1.0, December 2017. Available from: https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf [Accessed 22nd September 2020].
Training and Doctrine Command (TRADOC). (2018) *The US Army in Multi-Domain Operations 2028.* TRADOC Pamphlet 525-3-1. Available from: https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf [Accessed 10th August 2020].
Tucker, P.. (2019) *NATO Getting More Aggressive on Offensive Cyber.* Defense One, 24 May 2019. Available from: https://www.defenseone.com/technology/2019/05/nato-getting-more-aggressive-offensive-cyber/157270/ [Ac-

cessed 13th August 2020].
Underwood, K. (2020) *Army Shapes Joint All-Domain Operations.* AFCEA, 1 August 2020. Available from: https://www.afcea.org/content/army-shapes-joint-all-domain-operations [Accessed 14th August 2020].
US Joint Staff. (2018) *Memorandum for: Military Education Coordination Council Principals + Capstone Director.* Public Intelligence, 27 August 2018. Available from: https://publicintelligence.net/jcs-china-system-attack/ [Accessed 13th August 2020].
US Joint Staff. (2019) *Methodology for Combat Assessment.* CJCSI 3162.02. Washington, DC. 8 March 2019. Available from: https://www.jcs.mil/Portals/36/Documents/Doctrine/training/jts/cjcsi_3162_02.pdf?ver=2019-03-13-092459-350 [Accessed 14th August 2020].
Watling, J. & Roper, D. (2019) *European Allies in US Multi-Domain Operations.* Occasional Paper, Royal United Services Institute (RUSI). October 2019. Available from: https://rusi.org/sites/default/files/20190923_european_allies_in_us_multi-domain_operations_web.pdf [Accessed 13th August 2020].
Wijninga, E. (2018) *Training Joint Forces for Multi Domain Operations.* Conference read-ahead for the Joint Air & Space Power Conference 2019, Joint Air Power Competence Centre. Available from: https://www.japcc.org/training-joint-forces-for-multi-domain-operations/ [Accessed 22nd September 2020].
Williams, L. (2020) *JADC2 Tops Pentagon's Artificial Intelligence Efforts.* FCW, 9 July 2020. Available from: https://fcw.com/articles/2020/07/09/williams-jaic-ai.aspx [Accessed 13th August 2020].
Unal, B. (2019) *Cybersecurity of NATO's Space-Based Strategic Assets.* Chatham House, July 2019. Available from: https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf [Accessed 22nd September 2020].
Zadalis, T. (2018) Multi-Domain Command and Control: Maintaining Our Asymmetric Advantage. *Joint Air Power Competence Centre (JAPCC) Journal*. 26 (1). Available from: https://www.japcc.org/multi-domain-command-and-control/ [Accessed 13th August 2020].
Zager, R. & Zager, J. (2017) OODA Loops in Cyberspace: A New Cyber-Defense Model. *Small Wars Journal.* 21 October 2017. Available from: https://smallwarsjournal.com/jrnl/art/ooda-loops-cyberspace-new-cyber-defense-model [Accessed 2nd November 2020].

Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030

Franz-Stefan Gady
Research Fellow
Cyber, Space and Future Conflict Division
International Institute for Strategic Studies

Alexander Stronell
Research Assistant
Cyber, Space and Future Conflict Division
International Institute for Strategic Studies

Abstract: Synchronised kinetic and cyber operations across domains that present 'multiple dilemmas' are a fundamental tenet of multi-domain operations. Recent practice and study of the battlespace use of cyber capabilities in conjunction with kinetic operations, however, have shown the difficulties in creating joint effects due to insufficient synchronisation of operations or lack of coordination and control of cyber effects. This paper outlines three requirements needed to conduct integrated cyber and kinetic operations in a future high-intensity conflict involving NATO and a near-peer adversary: firstly, an internet of military things (IoMT) in conjunction with an artificial-intelligence (AI)-enabled command and control (C2) capability for integrated cyber and kinetic operations; secondly, multi-domain formations integrated with cyber commands or their respective organisational equivalents for coordinated theatre-wide cyber campaigns; and thirdly, a cyber mission command doctrine based on decentralised decision-making and decentralised execution to enable an accelerated operational pace. The analysis presents three comparative country studies— the US, UK and Germany— to assess the status of the integration of cyber capabilities into multi-domain warfighting concepts for high-intensity conflict in 2030. It also offers a preliminary set of recommendations on technical capabilities, new organisational structures and doctrinal changes required to facilitate the better integration of cyber with kinetic capabilities.

Keywords: *Offensive cyber operations, high-intensity warfare, multi-domain operations, internet of military things, mission command*

1. INTRODUCTION

Among NATO member states, the US has taken the lead in developing multi-domain operational concepts.[1] These are eventually expected to be adopted into formal doctrine in all military service branches and are built around synchronised combined arms operations across all five warfighting domains (including cyber and space); as well the electromagnetic spectrum. The US Army has designated its version of this new operational concept 'Multi-Domain Operations' (MDO) (TRADOC, 2018). The US Air Force, Navy, and Marine Corps are working on related concepts, and the Joint Chiefs of Staff are expected to publish a new overarching Joint Warfighting Concept for All-Domain Operations by the end of 2020 integrating the separate service approaches (Goure, 2019; Clark, 2020). The US' NATO allies, including the UK and Germany, have also begun the development of similar operational concepts (Kommando Heer, c.2017; Gerhartz, 2020).

Straddling all five warfighting domains,[2] cyberspace is not merely the connector of all systems, but also a weapons platform in itself, since cyberspace environments can be altered to allow for various vectors of attack on the adversary in ways that natural physical environments cannot. Synchronised kinetic and cyber operations across domains that present 'multiple dilemmas' are a fundamental tenet of multi-domain operations (Taylor & Kay, 2019).[3] Over the past decade, the US has pioneered the practical battlespace use of cyber capabilities in conjunction with kinetic operations, notably in operations conducted against Islamic State (also known as ISIL and ISIS). Though most details remain classified, US Cyber Command's Joint Task Force Ares (JTF-Ares), established in the first half of 2016, is known to have synchronised its capabilities with kinetic battlefield operations, most notably in Operation Glowing Symphony (OGS) (Martelle, 2018; Martelle, 2020), established to 'contest ISIL in the information domain'. Cyber Command has responsibility for coordinating its synchronisation with kinetic offensive operations conducted by other commands (US Cyber Command, 2016). Though characterised as a success, heavily redacted briefing documents suggest that significant challenges were encountered, and lessons learned in the deconfliction and engagement process. In particular, JTF-Ares cyberattack operators were required to undergo a further target vetting and deconfliction process after Combatant Command had formally designated a target for cyberattack, presumably complicating the engagement of time-sensitive targets (US Cyber Command, 2017; Martelle, 2020).

[1] No agreed definition of multi-domain operations among NATO member states exists. Multi-domain operations in this paper are defined as coordinated and synchronised combined arms operations across all warfighting domains and services at and above the tactical level that present multiple complementary threats to a great power adversary.

[2] No clear definition of domain exists among NATO member states (Townsend, 2019).

[3] For the sake of consistency, this paper will refer to all military operations built around synchronised combined arms operations across all five warfighting domains, the electromagnetic spectrum, and across service branches, as multi-domain operations and will use the MDO acronym only in reference to the US Army's narrower concept.

Several recent academic and military studies of the battlespace use of cyber capabilities in conjunction with kinetic operations demonstrate the difficulties associated with creating joint effects due to insufficient synchronisation of operations or lack of coordination and control of cyber effects (Metcalf & Barber, 2014; Kostyuk & Zhukov, 2017; Rothstein & Saltzman, 2019). A key challenge thus exists in the effective integration of conventional kinetic operations with cyber, space and information operations in the future battlespace. Further challenges identified as associated with multi-domain operations include the necessity of a secure and reliable cloud communication network; the need for highly trained personnel in command and control (C2); integration of allied capability; and stress exerted on the C2 structure (Rothstein & Saltzman, 2019).

Despite the apparent centrality of cyberspace to future high-intensity conflict, there has been little unclassified analysis of the specific technical, organisational and doctrinal requirements for the effective integration of cyber capabilities into multi-domain operations in future high-intensity warfighting scenarios (for some exceptions, see: Bonner, 2014; Reilly, 2016; McArdle, 2019; Rothstein & Saltzman, 2019). While literature exists exploring the organisational integration of offensive cyber capabilities (OIOCC) within national security structures (Smeets, 2018) and on kinetic and cyber operations in wartime (Kostyuk & Zhukov, 2017), the integration of kinetic and cyber strike capabilities for conventional warfighting has not formerly been addressed.

2. AIM

This paper will first analyse the conceptual origins of multi-domain operations before outlining the three requirements judged necessary for conducting integrated cyber and kinetic operations in a future high-intensity conflict involving NATO and a great power adversary in 2030: Firstly, an internet of military things (IoMT) in conjunction with an AI-enabled C2 capability for integrated cyber and kinetic operations; secondly, multi-domain formations integrated with cyber commands or their respective organisational equivalents for coordinated theatre-wide cyber campaigns; and thirdly, a cyber mission command doctrine based on decentralised decision-making and decentralised execution to enable an accelerated operational pace.

The analysis will then present three comparative country studies— the United States (US), United Kingdom (UK) and Germany—to assess the status of the integration of cyber capabilities based on the three identified requirements into multi-domain warfighting concepts for high-intensity conflict in 2030. These three countries were selected because they are among the largest military powers in the NATO alliance, and each publicly acknowledges the possession of offensive cyber capabilities. All three have also begun the development of operational concepts around or similar to multi-domain operations. The analysis will also offer recommendations on technical capabilities, new organisational structures, and doctrinal changes required to

facilitate the better integration of cyber with kinetic capabilities. The paper will not attempt to present a comprehensive set of capability requirements, nor will it address future multi-domain operations in their entire range and scope. Rather, it will confine itself to some of the technical, organisational and doctrinal capabilities judged to be necessary for the opening stages of a conventional high-intensity conflict between peers and near-peers after the breakdown of deterrence, and exclude what the Joint Chiefs of Staff (2019) refer to as 'competition below armed conflict' (Morris et al., 2019).

3. MULTI-DOMAIN OPERATIONS AND CYBER

The historical origins of the multi-domain operations warfighting concept are rooted in the US Army's AirLand Battle doctrine, first introduced in 1982 (Skinner, 1988). This multi-dimensional doctrine, updated in 1986 and 1993, focused on integrated, joint air and ground manoeuvre supported by long-range precision-guided munitions to defeat Soviet forces in Central Europe. NATO adopted the tenets of AirLand Battle for its Follow-On-Forces Attack Concept. AirLand Battle was considered an important contributing factor in the overwhelming allied victory during Operation Desert Storm in 1991 (Paquin, 1999), which was, in turn, instrumental in shaping the Chinese People's Liberation Army's (PLA) perception of future warfighting, triggering doctrinal changes and a concerted modernisation effort (Defense Intelligence Agency, 2019). However, Russian and Chinese military reforms in the 2000s—particularly the PLA's adoption of the 'informationised warfare' concept and Anti-Access/Area Denial (A2/AD) systems, Russian military modernisation efforts, and subsequent Russian operations in Ukraine in 2014—convinced US military leaders that AirLand Battle doctrine was obsolete. In 2015, Deputy Secretary of Defense Robert Work tasked the US Army with the development of 'AirLand Battle 2.0', which served as the institutional impetus to develop first the Multi-Domain Battle (MDB) concept and, subsequently, the MDO concept (McCoy, 2017; Johnson, 2018).

The importance of MDO for future NATO warfighting is twofold. Firstly, as the most comprehensive and advanced multi-domain concept of all US service branches, it is expected to constitute the foundational element of the new Joint Warfighting Concept for All-Domain Operations (Hoehn, 2020). Secondly, it is expected to influence the development of operational concepts and doctrine around multi-domain operations of NATO allies, in a similar manner to the influence of AirLand Battle on the Follow-On-Forces Attack Concept in the 1980s, although there are numerous capability gaps and policy challenges that need to be addressed first (Watling & Roper, 2019). According to the concept note, MDO has been developed to solve the problem of 'multiple layers of stand-off in all domains—and, sea, air, space and cyberspace — to separate US forces and our allies in time, space and function in order to defeat us'. The solution to this is:

> the rapid and continuous integration [emphasis added] of all domains of warfare to deter and prevail as we compete short

> of armed conflict. If deterrence fails, Army formations, operating as part of the Joint Force, penetrate and disintegrate enemy anti-access and area denial systems; exploit the resulting freedom of manoeuvre to defeat enemy systems, formations and objectives and to achieve our own strategic objectives; and consolidate gains to force a return to competition on terms more favourable to the U.S., our allies and partners (TRADOC, 2018: p. i, iii).

The underlying idea of MDO is thus deeper integration of capabilities across domains (also referred to as 'cross-domain synergy') to achieve convergence of time, space and capabilities to conduct independent manoeuvre and employ cross-domain fires including integrated kinetic and cyber strikes (TRADOC, 2018; Judson, 2020). Put otherwise, MDO is intended to accelerate the closing of the US Armed Forces' kill-chain, while simultaneously breaking the enemy's (Brose, 2020). Operational speed is vital in that regard and can only be guaranteed through the effective integration of separate battle networks into a system of systems architecture. Such an architecture will require sophisticated cyber defence and also narrow AI-enabled C2 capabilities to coordinate, deconflict and synchronise military operations across domains; for example, a coordinated and synchronised attack against an adversary C2 node via cyberspace, air and the electromagnetic spectrum. Cyberspace would thus not only be the key enabling domain for coordination and integration operations, but also an attack vector. Notably, in the US Air Force's Doolittle Series wargames, the centre of gravity for multi-domain operations was identified as the ability to create accurate and shared battlespace awareness, which, according to the joint force commander in the exercise, depended principally on protecting intelligence gathering systems and maintaining the security of C2 networks, both of which are dependent on cyberspace as their connector and integrator (Rothstein & Saltzman, 2019).

4. THREE REQUIREMENTS FOR EFFECTIVE INTEGRATION OF CYBER OPERATIONS INTO MULTI-DOMAIN OPERATIONS

There are numerous technical, organisational and doctrinal requirements necessary for the effective integration of cyber capabilities into multi-domain operations in future high-intensity warfighting scenarios. This section analyses the three judged to be most essential: an IoMT for effective cyber C2; integrated multi-domain formations; and a mission command doctrine based on decentralised decision-making and execution. All three countries discussed in this paper— the US, UK and Germany— are each working on at least one of the three requirements.

A. Technological

At the technological level, an IoMT is desired in combination with an AI-enabled C2 capability that enables the integration and synchronisation of cyber and kinetic strike capabilities in multi-domain operations. An IoMT is

a network or system of interconnected computing devices including sensors, weapons platforms, and data storage resources (Russell, Abdelzaher & Suri, 2019). It would thus theoretically collect and create vast amounts of shareable data, which could be turned into actionable intelligence for cyberattack packages. The IoMT would also enable the fast transfer of cyberattack packages to, for example, aircraft to target enemy air-gapped systems via the radio frequency (RF) spectrum (Theohary & Hoehn, 2019). The overall synchronisation and integration of operations in other domains would also require an AI-enabled C2 architecture also called an AI-enabled battle management system embedded within an IoMT capable of presenting a commander a real-time common operating picture that would include a cyber and electromagnetic picture. In essence, an AI-enabled battle management system in comparison to a conventional battle management system relies on machine-learning algorithms to process big data from multiple sources for C2 decision support in order to expedite the so-called dynamic observe, orient, decide, and act (DOODA) loop cycle (Schubert et al., 2018).

An IoMT paired with an AI-enabled C2 capability would thus fulfil a key requirement of multi-domain operations: information superiority in order to enable faster and more effective decision-making in the battlespace. As one analysis notes:

> Effective cross-domain data-driven decision-making relies on a precision balance between the right amount of information, the right amount of time and the correct ability to execute a choice. It is here where the [IoMT] complex system-of-systems can deliver benefit to all the phases of decision-making, regardless of context (Russell, Abdelzaher & Suri, 2019: p. 729).

An IoMT may also enable a faster closing of the cyber kill-chain. Using the seven phases of the Intrusion Kill-Chain Model, an IoMT would have its greatest utility in the reconnaissance phase or in the faster identification and selection of targets during multi-domain operations facilitated through a common cyber and electromagnetic picture (Hutchins, Cloppert & Amin, 2010). Nevertheless, there remain various technical and security challenges that need to be addressed before such a system can be operationalised, including cryptographic security and the power it consumes from devices (thereby reducing their lifespan) (Sfar et al., 2018; Eversden, 2020); military cloud computing architectures that may not meet the demand of real-time or near real-time battlefield awareness at the edge of a network, to which fog computing may present a solution (Butler, 2018); and the sheer scale of integration of large military formations (Kott, Swami & West, 2016).

B. Organisational

At the organisational level, the effective integration of kinetic and cyber strike capabilities in high-intensity warfighting scenarios will require the creation of multi-domain field formations which integrate battlespace intel-

ligence, surveillance, reconnaissance (ISR) assets such as unmanned combat aerial vehicles or low-earth orbit satellites with electronic and cyber warfare capabilities. This facilitates synchronised cyber operations in the tactical battlespace, and also fulfils the requirement of spatial proximity for tactical cyber operations via the RF spectrum (Schulze, 2020a). Theatre-wide cyber operations would require a delineation between tactical and strategic offensive cyber operations for battlespace management purposes. However, the multi-domain formation can be employed tactically or strategically. For example, a multi-domain unit could make use of either tactical or strategic intelligence assets (such as RF kit on the ground or a satellite) to gain access to a network and facilitate delivery of a cyber attack; and the effect achieved could also be either tactical or strategic. It may, for example, disrupt a surface-to-air battery or theatre-level C2. Conversely, while strategic offensive cyber operations would likely be authorised by national cyber commands elements of which could be embedded with a higher echelon formation, they could still be executed tactically. The multi-domain formation would also be responsible for cyber preparation of the battlespace; that is, it may perform activities akin to intelligence preparation of the battlespace, including the probing of enemy networks, assessment of cyber defences and the assembly of attack packages. Moreover, any cyber operation needs adequate preparation time. This is known as the 'cold-start' problem (Schulze, 2020a). As Matthias Schulze notes, offensive cyber operations, require:

> a huge logistical effort of keeping track of the status of implants and especially how different attack vectors are intertwined or depend on each other. High-value targets, such as critical infrastructures and command and control systems, are often air-gapped and require specialized intelligence to gain access. In many instances, this requires time-consuming social engineering in advance to gain a foothold on a system (Schulze, 2020a: pp. 188).

The successful integration of all cyber operations embedded within a multi-domain operating concept would be largely dependent on the close coordination of cyber operations between national cyber commands and tactical formations.

C. Doctrinal

At the doctrinal level, multi-domain operations require a mission command doctrine emphasising decentralised decision-making and decentralised pre-approved execution of integrated cyber strikes. Multi-domain operations, including offensive cyber operations, entail significant synchronisation and pre-planning. As several studies have noted, this can stand in fundamental tension with lower-level initiatives based on mission command as it prevents subordinates from seizing the initiative against the adversary at an opportune time in the battlespace:

> [if] the plan they [subordinates] are executing requires excessive synchronisation, then they will simply be unable to exploit these opportunities when they arise for fear of derailing the operation and preventing the convergence of effects' (Stafford, 2019: p. 96).

Should the technological capabilities for AI-enabled C2 sufficiently mature in the coming years, a mission command doctrine centred around decentralised planning and execution could nonetheless be realised under a multi-domain operating concept. In addition to an AI-enabled C2 ability to deconflict and synchronise operations across domains, key to an effective cyber mission command doctrine during multi-domain operations is pre-delegated authorisation to execute offensive cyberattacks at lower echelons of command. In a high-intensity warfighting environment, communication links to higher command or strategic cyber assets may be degraded and disrupted and individual commanders would have to have the appropriate C2 and authorisation to exploit opportunities in the cyber domain.

5. CASE STUDIES

The following three short case studies assess the current status of the three described technical, organisational, and doctrinal requirements for effective integration of offensive cyber capabilities into multi-domain operations.

A. United States

According to the forthcoming International Institute for Strategic Studies (IISS) comparative study of cyber military power, the US possesses the world's most advanced military offensive cyber capabilities. The US Armed Forces represent the primary driving force behind the adaptation of operational concepts based on multi-domain operations for high-intensity warfighting. It is thus unsurprising that it leads development in all three categories, and appears most advanced in integrating kinetic and cyber strike capabilities.

1) IoMT and AI-enabled C2 Capability

The US Department of Defense's (DoD) Joint All Domain Command and Control (JADC2) concept aims to integrate the separate tactical networks of the individual service branches of the US Armed Forces into one single network linking every sensor to every shooter across all levels in an IoMT. According to a recent Congressional briefing document, 'JADC2 envisions providing a cloud-like environment for the Joint force to share intelligence, surveillance and reconnaissance data, transmitting across many communications networks, to enable faster decision-making' (Hoehn, 2020). JADC2 envisions an AI-enabled C2 capability for military commanders similar to the ride-sharing service 'Uber' that provides real-time or near real-time situational awareness of the battlespace and lists available capabilities in all domains for the execution of mission sets. The DoD has tasked the US Air Force with delivering this technological capability in support of the JADC2 concept. For the

past two years, it has been working on its Advanced Battle Management System (ABMS), which, according to a senior service official, represents the first attempt by DoD to 'build the Internet of Things for the military' (Hitchens, 2020a; Rivers, 2020). ABMS consists of a set of six systems all concurrently under development, ranging from cloud-based C2 and situational awareness applications to sensor integration. ABMS has caused controversy with other service branches as a potential future C2 platform for all services; for example, the US Army raised a concern that it will face network scaling issues (Hitchens, 2020b). The US Government Accountability Office (GAO) has also raised concerns over ABMS technology and cost (US Government Accountability Office, 2020). Nonetheless, ABMS has shown initial some potential for multi-domain operations in a number of recent demonstrations, including providing AI-enabled C2 support and a real-time common operating picture—two key requirements for effective integration of offensive cyber and kinetic operations across domains. While the specifics regarding the testing have not been made public, reports suggest that they were part of scenarios (Tucker, 2020; Hitchens, 2020c).

2) Multi-Domain Formations

The US Army's concept note on MDO specifically calls for the creation of multi-domain formations capable of independent manoeuvre and the employment of cross-domain fires (TRADOC, 2018). In 2018, the Army stood up its first experimental Multi-Domain Task Force, the principal mission of which is the degradation and penetration of Chinese and Russian A2/AD bubbles (Freedberg, 2019). The heart of this task force is a new Intelligence, Information Operations, Cyberspace, Electronic Warfare and Space Operations (ICEWS) battalion capable of defensive and offensive cyber operations as well as 'converging signals intelligence and electronic warfare as an operational capability and space surveillance and effects' (Thompson, 2019). Notably, the battalion is not part of the joint Cyber Mission Force of US Cyber Command, but rather falls under US Army Cyber Command (2020). Both the Army and Marine Corps have been establishing stand-alone offensive cyber units as part of their new multi-domain warfighting approaches, while the Navy and Air Force continue to provide all of their offensive teams directly to Cyber Command (Pomerleau 2019a; 2019b). The Army is also reorganising or creating new cyber and electromagnetic activities planning sections at various headquarters, and standing up entire new units such as the 915th Cyber Warfare Support Battalion (Stover, 2020). A GAO report (2019) highlights 'staffing, equipping, and training challenges' within such units. It is unclear how precisely these new tactical units will integrate with the Cyber Mission Force under US Cyber Command, and precisely what offensive cyber capabilities they will have their disposal. Tactical and strategic offensive cyber capabilities will be coordinated via Joint Force Headquarters-Cyber and cyberspace operations integrated planning elements (CO-IPEs) attached to regional combatant commands (US Army War College, 2020). However, the exact mechanism including speed of decision-making for this is not publicly known.

3) Mission Command Doctrine and Decentralised Execution of Offensive Cyber Operations

According to the Joint Doctrine on cyberspace operations, 'The complex nature of [cyber operations], where cyberspace forces can be simultaneously providing actions at the global level and the theatre or joint operations area level, requires adaptations to traditional C2 structures' (Joint Chiefs of Staff, 2018). The document simultaneously emphasises that the mission command method of 'centralized planning with decentralized execution of operations' also applies to cyber operations. An overview of the current planning processes for joint offensive cyber operations suggests that it will remain fairly centralised in the near term at the upper echelons of command (US Army War College, 2020). This is gradually changing, however. National Security Presidential Memorandum 13, which governs the conduct of offensive and active defensive cyber operations under the doctrine of 'persistent engagement' (Pomerleau, 2019c; Nakasone, 2020), is enabling a more decentralised planning and execution of cyber operations below the strategic level (National Security Agency, 2012). Individual service branches have also been experimenting with the delegation of command authority to lower echelons (Pomerleau, 2018). However, this likely only pertains to more limited RF spectrum cyber operations, which would be closer to electronic warfare operations than strategic offensive cyber operations (US Army War College, 2020). According to the MDO concept note, national- (i.e. US Cyber Command) and theatre-level offensive cyberspace operations would converge at the corps level in the pursuit of operational and tactical objectives (TRADOC, 2018). C2 for offensive cyber operations would thus continue to reside at the highest level of military command, for example, with the corps commander and the geographical and functional combatant commanders (Hofer, 2019). This could make it difficult for field commanders below to exploit opportunities in cyberspace in a degraded operational environment using the mission command tenets should the MDO concept officially be adopted into doctrine.

B. United Kingdom

The UK's understanding of multi-domain operations closely resembles that of the US, though on a smaller scale. Facing greater budgetary and manpower constraints, the UK has focused its efforts on the development of an 'agile' and 'integrated' cyber capability under the umbrella of what it refers to as 'Multi-Domain Integration' (Ministry of Defence, 2017b; Connell, 2020; Stronell & Gady, 2020). The British Ministry of Defence's new Integrated Operating Concept, unveiled in September 2020, emphasises the need for integration across all warfighting domains at the tactical level (Ministry of Defence, 2020a). According to the Ministry of Defence (2017a: p.1), British 'military activities increasingly need to incorporate the often subtle and ambiguous interplay between cyber electromagnetic and information activities which must be integrated, as required, with kinetic effects'. British officials have repeatedly acknowledged the challenge presented by multi-domain operations and there is significant evidence of adaptation within the British armed forces to the challenges presented (Carter, 2019; Sanders 2020).

1) IoMT and AI-Enabled C2 Capability

Statements by British officials and defence research institutions have recognised the importance both of an IoMT and AI-enabled C2 capability to the future multi-domain battlespace, though the development of capability appears to remain in the experimental stage in most cases (Poulter & Mackay, 2018; Royal Air Force, c.2020). There is no dedicated programme to create a battle management system integrating the separate service branches and their systems and platforms in an IoMT underpinned by AI-enabled C2 capability. However, the UK is in the process of developing a large-scale AI-enabled synthetic environment in order to aid in the development of course-of-action analysis. Such a tool could eventually evolve into an operational tool for such an AI-enabled C2 (The Economist, 2019; Warrell, 2020).

Overall, IoMT developments appear to remain relatively fragmented and platform-centred. One key focus is the development of the Future Combat Air System (FCAS) system-of-systems concept, headed by BAE Systems' Tempest, which seeks to connect sensors and shooters into an IoMT and includes the development of an 'air combat cloud' (Harper, 2019). In its Integrated Review and Air Space Proposition, the Royal Air Force (c.2020) emphasises that an IoMT that fuses and distributes data across domains is at the heart of its modernisation efforts: '[b]y harnessing information, fusing data on a cross-domain network of interconnected systems, we will achieve advantage over our adversaries and competitors'. The 'Intelligent Ship' programmes, funded by the UK's defence innovation accelerator, represent another example. One project aim is to 'enable integration and application of intelligence systems' while another is to develop and understand how 'complex networks of humans and machines can effectively team' (DASA, 2019). Both objectives seek to support an AI-enabled C2 capability. The UK Strategic Command has also championed the Integrated Warrior programme which seeks to work with academia and industry to develop new force structures, capabilities and new operating concepts for the future operating environment (Royal Navy, 2020).

2) Multi-Domain Formations

Three main institutional innovations characterise the UK's response to multi-domain operations. UK Strategic Command, established in February 2020, represents the most fundamental of these. Assuming the role of 'defence integrator', the Command's key innovation in relation to its predecessor is its aspiration to more effectively integrate cyber and space capabilities with the three classical warfighting domains, and to achieve seamless planning and execution of multi-domain operations at a pace that outstrips the UK's adversaries (Barry, 2020). Strategic Command succeeds UK Joint Forces Command, itself established in 2012 to integrate British key strategic level military capabilities more effectively. Official statements have repeatedly referred to the new Command as the British response to multi-domain challenges (Curtis 2019; Ministry of Defence, 2019b; 2020c; Sanders, 2020).

The UK National Cyber Force, which combines the cyber capabilities of the UK's technical intelligence agency, Government Communication Headquarters (GCHQ), with those of the Ministry of Defence also represents a relatively new innovation which is likely to assist the UK in multi-domain operations. By combining its military and intelligence cyber capabilities, the UK hopes to attain significant agility in cyberspace operations. As such, the role of Cyber Force is conceived very differently to that of US Cyber Command, intended to overcome inter-agency rivalry and the splintering of cyber capabilities across government present in the American system. Instead, different operations conducted by Cyber Force will fall under the purview of either the intelligence services or the military, depending on the nature of the operation (Stronell & Gady, 2020). Work towards the Force having first been announced in 2018, it is likely in the process of achieving institutional maturity, with its official inauguration likely to be announced in the coming months (The Telegraph, 2018; Sabbagh, 2020; Stronell & Gady, 2020).

The British Army's 6th Division, formed in August 2019, represents a third institutional response to multi-domain operations. The division, which replaced the combat support Force Troops Command, has been dubbed the British Army's 'hybrid warfare' branch by the media (Sengupta, 2019). Intended to provide the British Army with greater capability to defeat adversaries both above and below the threshold of conventional conflict, press releases describe the Division, which represents approximately one-fifth of the UK's Field Army, as tasked with 'cyber, electronic warfare, intelligence, information operations and unconventional warfare' (Ministry of Defence, 2019b; Warfare Today, 2019). The unit also includes the British Army's first 'cyber regiment', which appears to have capabilities for offensive cyber operations (Chuter, 2020). It is unclear how precisely the new unit will integrate with the National Cyber Force.

3) Mission Command Doctrine and Decentralised Execution of Cyber Operations

The British vision of 'Multi-Domain Integration' encompasses not only the three-armed services, but allied capabilities and civilian government organisations including the intelligence services. Capability integration, particularly at the national level, is seen as a force multiplier (Ministry of Defence, 2020a). According to the joint British doctrine for cyber and electromagnetic activities (CEMA), the British military envisions the integration of CEMA into the wider military as part of a full-spectrum approach (Ministry of Defence, 2018). There has been a progressively increased doctrinal emphasis on capability integration (including cyber and space) across the past several editions of capstone British doctrine and the latest joint doctrine note on cyber and electromagnetic activities emphasises the need for a cyber electromagnetic picture as part of a common operating picture to support future military operations for combined kinetic and cyber operations (Ministry of Defence, 2008; 2011; 2014; 2018). The UK is clearly turning its doctrinal focus to the development of a force structure compatible with this multi-domain, integrated operational concept (Sanders, 2020). The publication of the Integrated Operating Concept 2025 sheds considerable light on how the Brit-

ish government envisions the integration and use of UK cyber capabilities in multi-domain operations, anticipating integration of capabilities at the tactical as well as the operational level of war. The doctrine envisions an operational concept 'integrated across all five Operational Domains [...which] will change the way we operate and war fight and the way we develop capability' (Ministry of Defence, 2020a).

Mission command and decentralised execution of offensive cyber strikes were both used during operations against terrorist organisations (Blitz, 2013; Bond, 2018; Stronell & Gady, 2020). In a concept note on future C2 design, the Ministry of Defence (2017a: p.6) stresses that it has to meet the 'enduring requirement for mission command'. However, in a key point of departure from US practice, British practitioners possess an engrained scepticism of the necessity of granting the autonomy to launch cyber operations to tactical-level units. There is also an overall resistance to the tactical-strategic distinction as regards the prosecution of cyber operations. British officials are likely hopeful that an integrated national capability can provide the necessary tactical-level support to troops on the ground while maintaining the ability to achieve strategic effects. In keeping with longstanding British practice, authorisation for the prosecution of cyber operations (either individually or collectively) will likely remain with government ministers; namely, with the Foreign Secretary in peacetime and the Secretary of State for Defence in conflict situations (Stronell & Gady, 2020).

C. Germany

No operating concept around multi-domain operations yet exists in the German armed forces (Bundeswehr). The basic tenets of multi-domain operations, however, have been outlined in various official documents discussing future warfighting and force modernisation (Kommando Heer, 2018). Indeed, according to a Bundeswehr official, multi-domain operations are an integral part of operational planning within the armed forces (Gady, 2020b). While the Bundeswehr Cyber and Information Domain Service possesses a burgeoning offensive cyber military capability, there is little publicly available information about efforts to integrate cyber and kinetic strike capability for high-intensity warfare.

1) IoMT and AI-enabled C2 Capability

An IoMT and AI-enabled C2 capability remain aspirational for the Bundeswehr for the time being. While it has identified an IoMT as part of a set of capabilities needed for generating 'AI-supported quality data' as part of its digitalisation strategy for German land forces (Bundeswehr, 2020: p.2), no funded programme has yet been established. In the near term, German efforts (in collaboration with the Netherlands) for a new battle management system are focused on the Tactical Edge Network (TEN) programme, which is expected to enter service with the German Army in 2023 (Leidenberger et al., 2020). The underlying battle control software, SitaWare Frontline, is not AI-enabled (Defense-Aerospace, 2019). According to state-owned IT service provider BWI, TEN will be a building block of the IoMT and a sensor-to-

shooter concept, which will presumably include an AI-enabled C2 capability (Leidenberger et al., 2020). It remains unclear to what degree there are plans to integrate the Bundeswehr Cyber and Information Domain Service, including its offensive cyber capabilities, into such an IoMT. The Bundeswehr has historically encountered difficulties in creating a joint operating picture across services, let alone domains (Dyson, 2011). Within the Cyber and Information Domain Service, however, some AI-enabled operating picture capabilities have been in development since 2016 (BWI, 2020). For the time being, IoMT efforts appear fragmented and platform-focused. For example, in cooperation with Spain and France, Germany is co-developing the Future Combat Air System (FCAS), a system-of-systems (an IoMT) underpinned by a tactical cloud, with an AI-enabled C2 capability (Gros, 2019). The FCAS is expected to enter service in the 2040s. In cooperation with France, Germany is also developing a Main Ground Combat System—a multiplatform concept based on a system-of-systems architecture expected to be deployed in the mid-2030s. Overall, there appears to be no coordinated technological-level effort towards the integration of cyber and kinetic strike capabilities for multi-domain operations set in a high-intensity warfighting scenario within the Bundeswehr.

2) Multi-Domain Formations

The Bundeswehr has not established any multi-domain formations for conducting offensive cyber operations, and according to the Cyber and Information Domain Service, there are no existing plans to deploy such formations in the future (Gady, 2020a). Germany only recently established an independent military cyber force, the Bundeswehr Cyber and Information Domain Service, which became operational in 2017, and is loosely modelled on US Cyber Command and its cyber forces. The service consolidates around 14,000 civilian and military personnel divided up into various units and commands, with the majority of formations consisting of electronic warfare and IT-support battalions. Military cyber capabilities are situated within the Centre for Cyber Defence and Centre for Cyber Operations, which is also responsible for conducting offensive cyber operations. The eventual manpower of these two centres is expected to reach 600, with around 100 civilian and military personnel assigned to the Centre for Cyber Operations (Bundesministerium der Verteidigung, 2016; Gady, 2020b). The Bundeswehr intends to deploy Cyber-Information-Domain (CID) teams with individual services and units to act as liaisons and advisors to military commanders. Offensive cyber operations, however, would still be centrally executed through the 'Reach-Back-Verfahren' (reach back procedure) by the Cyber and Information Domain Service (Gady, 2020a). According to a statement by the German Defence Ministry, the main objective of offensive cyber operations will be the attainment of 'information dominance' in the cyber and information spaces to support an accelerated decision-making cycle during kinetic operations (Bundesministerium der Verteidigung, 2017). One likely reason for the absence of multi-domain formations akin to the US Army's cyber battalions or the British Army's 'cyber regiment' is that a Bundeswehr cyber unit would suffer from limited utility at the outset of any high-intensity warfighting

scenario since it would likely be legally difficult to conduct cyber preparations of the battlespace without the direct authorisation of the German parliament before the outbreak of hostilities (Schulze, 2020c). While under emergency situations parliamentary consent to military operations can be given retroactively (as long as this is preceded by informing select members of the Bundestag's Defence Committee), it is unclear whether this could apply to cyber preparations of the battlespace, which could require many months of runup time prior to the commencement of hostilities.

3) Mission Command Doctrine and Decentralised Execution of Offensive Cyber Operations

Germany does not possess an official cyber military doctrine. According to recent research, doctrinal discussions on the use of offensive cyber capabilities are found in various government documents, but they are generally vague and offer little guidance about their deployment (Schulze, 2020b). In comparison to British and American legislative institutions, the Bundestag enjoys extended powers over operational matters, including rules of engagement and C2 (Dyson, 2011), underscoring the inhibited decision-making autonomy of the Bundeswehr in the cyber domain. Strong civilian oversight also incentivises more direct control of offensive cyber operations by higher echelons of military command within the armed forces. This stands in tension with the Bundeswehr Networked Operational Command Doctrine (Vernetzte Operationsführung), which aims to create a networked warfighting approach underpinned by mission command (Bundesministerium der Verteidigung, 2017). According to one 2011 study exploring the digitisation of the Bundeswehr, 'the practical experience of digitisation in exercises has led to the temptation for commanders to involve themselves in the 'tactical weeds' [and] networking has been accompanied by enhanced accountability'. The result, according to the study, is that tactical decisions are taken at higher echelons of command. Referring to actual operational experiences from Afghanistan, the study further notes that 'commanders are gathering inappropriate levels of information and are being pulled down to the detailed tactical level, to protect themselves from prosecution' (Dyson, 2011: p.7). All these factors will likely make it very difficult for German commanders to apply mission command, seize the initiative, and exploit opportunities in the battlespace through the combined use of kinetic and cyber capabilities during multi-domain operations. Nonetheless, according to the Cyber and Information Domain Service, cyber operations will be conducted by applying the tenets of mission command (Gady, 2020a). However, the service does caution that the specific characteristics of cyber operations need to be considered.

6. IMPLICATIONS FOR NATO

The three case studies assessing technical, organisational and doctrinal requirements for the effective integration of cyber and kinetic strike capabilities into multi-domain operational concepts in a high-intensity conflict yield several practical conclusions for the NATO alliance.

Firstly, as all three case studies illustrate, the integration of cyber and kinetic capabilities for multi-domain operations remains largely aspirational and at an experimental stage. Little public information exists about precisely how the armed forces of the three countries would execute synchronised cyber-kinetic strikes in a high-intensity conflict. The difficulties of effectively coordinating offensive cyber-kinetic strikes during multi-domain operations implies that they may principally be employed at the outset of a high-intensity conflict for high-value targets such as an enemy's national or theatre-wide C2 networks. Another contributing factor is the 'cold start' problem, and the need for adequate cyber preparation of the battlespace and possible quick depletion of cyber weapons arsenals (for example, malware and 0-day vulnerabilities). Consequently, NATO should have an enhanced focus during wargames and exercises on the initial stages of multi-domain operating in a high-intensity warfighting environment, and must consider to what degree and how offensive cyber capabilities are to be used by military commanders (Schneider, 2017).

Secondly, NATO needs to develop its own, separate doctrine on multi-domain operations. The US is leading the conceptual development of multi-domain operations, but allies must follow suit to adapt the concept to their own future capabilities, resources and requirements. The UK and Germany are in the early stages of doctrinal development, though the former is at a far more advanced stage. Nevertheless, separate national efforts will only go so far, and may impede unity of effort. To facilitate effective integration and interoperability between NATO member states, a clear doctrinal foundation for multi-domain operations should be developed. This would also assist in identifying and prioritising capability requirements among member states for the execution of multi-domain operations. A new multi-domain doctrine would also likely require updates to NATO's *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations* (NATO, 2020). In particular, it would require revision of the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism for offensive cyber operations (ibid.; Goździewicz, 2019).

Thirdly, clear technical requirements and standards for a common systems architecture that enables integration of separate battle management systems need to be established across NATO member states. Only a secure and interconnected battle management system paired with an AI-enabled C2 capability that includes a common cyber electromagnetic picture will be able to effectively integrate kinetic and cyber operations in a high-tempo warfighting environment. Such an effort could be modelled on NATO's Air Command and Control System Programme, or expand on the Dutch-German TEN programme (NATO, 2015). Different capabilities among NATO member states, the cost associated with multi-domain C2 systems, and classification challenges encountered when operating across NATO particularly with regards to cyber operations will make the integration of separate battle management systems a difficult proposition. Given that multi-domain operations inherently involve dependence on technological capabilities, strong AI-enabled cyber defences across the alliance will be an absolute necessity.

Fourthly, as the German case study clearly demonstrates, legal restrictions and domestic political considerations could prevent the effective use of multi-domain formations and offensive cyber operations in high-intensity conflict. Offensive cyber operations require preparation of the battlespace, which may be legally prohibited without a parliamentary mandate. To effectively execute synchronised operations under mission command principles would also require authorisation at lower echelons of command. Neither Germany nor the UK, however, appear eager to decentralise decision-making as regards the use of offensive cyber capabilities. Consequently, the alliance should encourage member states to specify detailed legal requirements for the execution of offensive cyber operations at all levels of command.

7. REFERENCES

Barry, B. (2020) 'New UK Strategic Command faces early challenges'. Military Balance blog, 19th June. London, International Institute for Strategic Studies. Available at: https://www.iiss.org/blogs/military-balance/2020/06/uk-strategic-command-challenges-covid-19 [Accessed: 1st August 2020].

Blitz, J. (2013) 'UK becomes first state to admit to offensive cyber-attack capability'. *Financial Times*, 29th September. Available at: https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de [Accessed: 1st August 2020].

Bond, D. (2018). 'UK reveals Isis target of first military cyber-attack'. *Financial Times*, 12th April. Available at: https://www.ft.com/content/cea9d608-3e3f-11e8-b7e0-52972418fec4 [Accessed: 1st August 2020].

Bonner, E. (2014) 'Cyber Power in 21st-Century Joint Warfare'. *Joint Force Quarterly*, 74, 3rd Quarter, 102-109. Available from: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-74/jfq-74_102-109_Bonner.pdf [Accessed: 1st August 2020].

Brose, C. (2020) *The Kill Chain: Defending America in the Future of High-Tech Warfare*. New York NY, Hachette Books.

Bundesministerium der Verteidigung. (2017) 'Strategische Leitlinie Digitalisierung'. Government report, March. Available at: https://www.bundeswehr.de/resource/blob/66394/4bbd6bd8e0fe81df975480a081bd1a37/20190703-strategische-leitlinie-digitalisierung-data.pdf [Accessed: 1st August 2020].

Bundesministerium der Verteidigung. (2016) 'Abschlussbericht Aufbaustab Cyber- und Informationsraum'. Government report, April. Available at: http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf [Accessed: 1st August 2020].

Bundeswehr. (2020) 'Strategie Digitalsierung Land: Ein „DO IT-System für Entscheider'. Available at: https://www.bundeswehr.de/resource/blob/164082/597926df1b0c7941f755dda7589f1fc9/faltblatt-strat-digl-data.pdf [Accessed: 1st August 2020].

Butler, B. (2018) 'What is fog computing? Connecting the cloud to things.' *Network World*, 17th January. Available at: https://www.networkworld.com/article/3243111/what-is-fog-computing-connecting-the-cloud-to-things.html [Accessed: 1st August 2020].

BWI. (2020) 'Von Big Data bis KI – Bundeswehr und BWI starten zweite Ausbaustufe des Gemeinsamen Lagezentrums CIR'. Blog, 1st September. Available at: https://www.bwi.de/news-blog/news/artikel/von-big-data-bis-ki-bundeswehr-und-bwi-starten-zweite-ausbaustufe-des-gemeinsamen-lagezentrums-cir [Accessed: 2nd September 2020].

Carter, N. (2019) 'Chief of the Defence Staff [...] annual RUSI speech'. Speech transcript, 5th December. London, Ministry of Defence. Available at: https://www.gov.uk/government/speeches/chief-of-the-defence-staff-general-sir-nick-carters-annual-rusi-speech [Accessed: 1st August 2020].

Chuter, A. (2020). 'British Army launches its first cyberwar regiment'. Defense News, 4th June. Available at: https://www.defensenews.com/global/europe/2020/06/04/british-army-launches-its-first-cyberwar-regiment/ [Accessed: 1st August 2020].

Clark, C. (2020) 'Gen. Hyten on the New American Way of War: All-Domain Operations'. *Breaking Defense*, 18th February. Available from: https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/ [Accessed: 1st August 2020].

Connell, S. (2020) 'Why protecting our nation is only possible through better collaboration'. Blog, 15th September. Northwood, UK Strategic Command. Available at: https://stratcommand.blog.gov.uk/2020/09/15/why-protecting-our-nation-is-only-possible-through-better-collaboration/ [Accessed: 15th September 2020].

Curtis, A. (2019) 'Joint Forces Command to Become Strategic Command'. Commentary, 6th August. London, Royal United Services Institute. Available at: https://www.rusi.org/commentary/joint-forces-command-become-strategic-command [Accessed: 1st August 2020].

Defence and Security Accelerator [DASA]. (2019) 'Competition document: intelligent ship - the next generation'. London, Ministry of Defence, 15th July. Available at: https://www.gov.uk/government/publications/competition-intelligent-ship-the-next-generation/competition-document-intelligent-ship-the-next-generation [Accessed: 1st August 2020].

Defense Intelligence Agency. (2019) *China Military Power: Modernizing a Force to Fight and Win*. Washington DC, Department of Defense. Available from: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf [Accessed: 1st August 2020].

Defense-Aerospace. (2019) 'SitaWare Frontline Chosen by German Armed Forces as BMS for VJTF(L) 2023'. *Systematic* press release, 12th December. Available at: https://www.defense-aerospace.com/articles-view/release/3/208209/bundeswehr-chooses-systematic-c2-software-for-vjtf.html [Accessed: 1st August 2020].

Deployable Training Division of the Joint Staff J7. (2020). *Mission Command*, January. Second edition. Insights and Best Practices Focus Paper. Suffolk VA, Joint Chiefs of Staff. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/missioncommand_fp_2nd_ed.pdf?ver=2020-01-13-083451-207 [Accessed: 1st August 2020].

Dyson, T. (2011) 'Managing Convergence: German Military Doctrine and Capabilities in the 21st Century'. *Defence Studies*, June. 11 (2), 244-270. Available at: https://core.ac.uk/download/pdf/397643.pdf [Accessed: 1st August 2020].

Eversden, A. (2020) 'DARPA wants stronger security for Internet of Things devices,' 12th August. *C4ISRNET*. Accessed at: https://www.c4isrnet.com/

battlefield-tech/it-networks/2020/08/12/darpa-wants-stronger-security-for-internet-of-things-devices/ [Accessed: 1st September 2020].

Freedberg Jr., S. (2019) 'Army's Multi-Domain Unit 'A Game-Changer' In Future War'. *Breaking Defense*, 1st April. Available at: https://breakingdefense.com/2019/04/armys-multi-domain-unit-a-game-changer-in-future-war/ [Accessed: 1st August 2020].

Gady, F. (2020) Interview with German Cyber and Information Domain Service spokesperson, 25th September.

Gady, F. (2020) Interview with Bundeswehr spokesperson, 16th August.

Gerhartz, I. (2020) 'The Luftwaffe in Multi-Domain Operations'. *Journal of the JAPCC*. 30. Available at: https://www.japcc.org/the-luftwaffe-in-multi-domain-operations/ [Accessed 1st October 2020].

Goure, D. (2019) 'A New Joint Doctrine for an Era of Multi-Domain Operations'. *Real Clear Defense* [via TRADOC], 11th October. Available from: https://www.tradoc.army.mil/Publications-and-Resources/Article-Display/Article/1987883/a-new-joint-doctrine-for-an-era-of-multi-domain-operations/ [Accessed: 1st August 2020].

Government Accountability Office [GAO]. (2020) 'Defense Acquisitions: Action Is Needed to Provide Clarity and Mitigate Risks of the Air Force's Planned Advanced Battle Management System'. Report to Congressional Committees GAO-20-389 April. Washington DC. Available at: https://www.gao.gov/products/GAO-20-389 [Accessed: 1st August 2020].

Government Accountability Office [GAO]. (2019) 'Future Warfare: Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping and Training of New Organizations'. Report to Congressional Committees GAO-19-570, August. Washington DC. Available at: https://www.gao.gov/products/gao-19-570 [Accessed: 1st October 2020].

Goździewicz, W. (2019) 'Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)'. *Cyber Defense Magazine*, 11th November. Available at: https://www.cyberdefensemagazine.com/sovereign-cyber/ [Accessed: 1st October 2020].

Gros, P. (2019) 'The "tactical cloud", a key element of the future combat air system'. Note 19/19, 2nd October. Paris, Fondation pour la recherche stratégique. Available at: https://www.frstrategie.org/en/publications/notes/tactical-cloud-key-element-future-combat-air-system-2019.

Harper, J. (2019) 'What to Expect from Sixth-Gen Aircraft'. *National Defense*, 16th September. Available at: https://www.nationaldefensemagazine.org/articles/2019/9/16/what-to-expect-from-sixth-gen-aircraft [Accessed: 1st August 2020].

Hitchens, T. (2020) 'ABMS Demos Speed New Capabilities to Warfighters'. *Breaking Defense*, 21st January. Available from: https://breakingdefense.com/2020/01/abms-demos-speed-new-capabilities-to-warfighters/ [Accessed: 1st August 2020].

Hitchens T. (2020) 'MDO Exclusive: Air Force Targets Primary Role in Joint C2'. *Breaking Defense*, 21st January. Available at: https://breakingdefense.com/2020/01/mdo-exclusive-air-force-targets-primary-role-in-joint-c2/ [Accessed: 1st August 2020].

Hitchens, T. (2020) 'ABMS Demo Proves AI Chops for C2'. *Breaking Defense*, 3rd September. Available at: https://breakingdefense.com/2020/09/abms-demo-proves-ai-chops-for-c2/ [Accessed: 5th September 2020].

Hoehn, J. (2020) 'Joint All Domain Command and Control (JADC2)'. Congressional briefing paper, 25th August. Washington DC, Congressional Research Service. Available at: https://fas.org/sgp/crs/natsec/IF11493.pdf [Accessed: 1st September 2020].

Hoehn, J. & Theohary, C. (2019) 'Convergence of Cyberspace Operations and Electronic Warfare'. Congressional briefing paper, 13th August. Washington DC, Congressional Research Service. Available at: https://fas.org/sgp/crs/natsec/IF11292.pdf [Accessed: 1st August 2020].

Hofer, M. (2019) 'The C2 of Cyberspace is a Mess!' *Proceedings of the US Naval Institute*, August. 145 (8). Available at: https://www.usni.org/magazines/proceedings/2019/august/c2-cyberspace-mess [Accessed: 1st September 2020].

Hutchins, E., Cloppert, M. & Amin, R. (2010) 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains' Lockheed Martin. Available at: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [Accessed: 2nd October 2020].

Johnson, D. (2018) 'Shared Problems: The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle' Santa Monica CA, RAND Corporation, August. Available at: https://www.rand.org/pubs/perspectives/PE301.html [Accessed: 1st October 2020].

Joint Chiefs of Staff. (2019) 'Competition Compendium'. Joint Doctrine Note 1-19, 3rd June. Available from: https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf [Accessed: 1st August 2020].

Joint Chiefs of Staff. (2018) *Cyberspace Operations*, 8th June. Joint Publication 3-12. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf [Accessed: 1st August 2020].

Judson, J. (2020) 'Inside Project Convergence: How the US Army is preparing for war in the next decade'. *Defense News*, 10th September. Available at: https://www.defensenews.com/smr/defense-news-conference/2020/09/10/army-conducting-digital-louisiana-maneuvers-in-arizona-desert/ [Accessed: 15th September 2020].

Kommando Hier. (c.2018) 'Digitalisierung von Landoperationen'. Thesenpapier [Research Paper]. Available at: https://www.dwt-sgw.de/fileadmin/redaktion/SGW-Veranstaltungen/2018/8F7_Landoperationen/Thesenpapier_II_Digitalisierung_Landoperationen.pdf?fbclid=IwAR2_EkjXYoK-kQbMHNArC-K7ecyvjfCQfqQHXaAk80ITTnNE2rDckHttWsAI [Accessed: 1st August 2020].

Kommando Heer. (c.2017) 'Wie kämpfen Landstreitkräfte künftig?' Thesenpapier [Research Paper]. Available from: https://www.pivotarea.eu/wp-content/uploads/2017/09/OOO.pdf [Accessed: 1st August 2020].

Kostyuk, N. & Zhukov, Y. (2017) 'Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?' *Journal of Conflict Resolution*. 63 (2), 317-347. Available from: https://journals.sagepub.com/doi/abs/10.1177/0022002717737138 [Accessed: 1st August 2020].

Kott, A., Swami, A., West, B. (2016) 'The Internet of Battle Things'. *IEEE Computer*. 49 (12), 70-75. Available at: https://arxiv.org/ftp/arxiv/papers/1712/1712.08980.pdf [Accessed: 1st August 2020].

Leidenberger, F., Trampert, M., Bonnen, H. & Haber, T. (2020) 'BWI – Unterstützer der Digitalisierung der Bundeswehr'. *Wehrtechnische Report*. 17-19. Available at: https://esut.de/wp-content/uploads/2020/05/IT_REPORT_2020.pdf [Accessed: 1st September 2020].

Martelle, M. (2020) 'USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY'. Briefing Book 693 21st January. Washington DC, National Security Archive. Available at: https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony [Accessed: 1st October 2020].

Martelle, M. (2018) 'Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL'. Briefing Book 637 13th August. Washington DC, National Security Archive. Available at: https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil [Accessed: 1st October 2020]

McCoy, K. (2017) 'The Road to Multi-Domain Battle: An Origin Story'. West Point NY, Modern War Institute at West Point, 27th October. Available at: https://mwi.usma.edu/road-multi-domain-battle-origin-story/ [Accessed: 1st August 2020].

Metcalf, A. & Barber, C. (2014) 'Tactical Cyber: How to Move Forward'. *Small Wars Journal*, 14th September. Available from: https://smallwarsjournal.com/jrnl/art/tactical-cyber-how-to-move-forward [Accessed: 1st August 2020].

Ministry of Defence. (2020) 'The Integrated Operating Concept 2025,' 30th September. Available at: https://www.gov.uk/government/publications/the-integrated-operating-concept-2025 [Accessed: 1st October 2020].

Ministry of Defence. (2020) 'HMS TAMAR and RAF WYTON Read Outs'. Press release, 16th September. London, Directorate Defence Communications [email].

Ministry of Defence. (2020) 'Visions for Strategic Command outlined during inaugural RUSI Conference'. Press release, 20th February. Available at: https://www.wired-gov.net/wg/news.nsf/print/Visions+for+Strategic+Command+outlined+during+inaugural+RUSI+Conference+20022020151515 [Accessed: 1st August 2020].

Ministry of Defence. (2019) 'Joint Forces Command to Strategic Command, the journey'. Press release, 9th December. Northwood, UK Strategic Command. Available at: https://www.gov.uk/government/news/joint-forces-command-to-strategic-command-the-journey [Accessed: 1st August 2020].

Ministry of Defence. (2019) 'Army restructures to confront evolving threats'. Press release, 1st August. Available at: https://www.gov.uk/government/news/army-restructures-to-confront-evolving-threats [Accessed: 15th August 2020].

Ministry of Defence. (2018) 'Cyber and Electromagnetic Activities'. Joint Doctrine Note 1/18, February. Shrivenham, Development, Concepts and Doctrine Centre. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf [Accessed: 1st August 2020].

Ministry of Defence. (2017) 'Future of Command and Control'. Joint Concept Note 2/17, September. Shrivenham, Development, Concepts and Doctrine Centre. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643245/concepts_uk_future_c2_jcn_2_17.pdf [Accessed: 10th September 2020].

Ministry of Defence. (2017) 'Future Force Concept'. Joint Concept Note 1/17, July. Shrivenham, Development, Concepts and Doctrine Centre. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/

uploads/attachment_data/file/643061/concepts_uk_future_force_concept_jcn_1_17.pdf [Accessed: 1st August 2020].

Ministry of Defence. (2014) 'UK Defence Doctrine'. Joint Doctrine Publication 0-01, November. Shrivenham, Development, Concepts and Doctrine Centre. Fifth edition. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf [Accessed: 1st August 2020]

Ministry of Defence. (2011) 'British Defence Doctrine'. Joint Doctrine Publication 0-01, November. Shrivenham, Development, Concepts and Doctrine Centre. Fourth edition. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf [Accessed: 1st August 2020].

Ministry of Defence. (2008) 'British Defence Doctrine'. Joint Doctrine Publication 0-01, August. Shrivenham, Development, Concepts and Doctrine Centre. Third edition.

Morris, L., Mazarr, M., Hornung J., Pezard, S., Binnendijk, A. & Kepe, M. (2019) *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*. Santa Monica CA, RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RR2942.html [Accessed: 1st August 2020].

Nakasone, P. & Lewis, C. (2017) 'Cyberspace in Multi-Domain Battle'. *The Cyber Defense Review*. 2 (1), 15-26. Available from: https://www.jstor.org/stable/26267397 [Accessed: 1st August 2020]

Nakasone, P. (2020) 'Statement of [...] Commander United States Cyberspace Command before the House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities,' 4th March. Washington DC, United States Congress. Available at: https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf [Accessed: 1st August 2020].

National Security Agency [NSA]. (2012) 'Presidential Policy Directive 20'. PPD-20. Washington DC, Department of Defense. Available at: https://fas.org/irp/offdocs/ppd/ppd-20.pdf [Accessed: 1st August 2020].

NATO. (2020) *AJP-3.20: Allied Joint Doctrine for Cyberspace Operations*. Edition A. Version 1, January. Brussels. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf. [Accessed 24th November 2020].

NATO. (2015) 'NATO Air Command and Control System (ACCS)' 24th September. Available at: https://www.nato.int/cps/en/natohq/topics_8203.htm [Accessed: 1st August 2020].

Paquin, R. (1999) 'Desert Storm: Doctrinal AirLand Battle Success or "The American Way of War"'. Monograph. Fort Leavenworth KS, School of Advanced Military Studies, United States Army Command and General Staff College. Available from: https://apps.dtic.mil/dtic/tr/fulltext/u2/a370380.pdf [Accessed: 1st August 2020].

Pomerleau, M. (2019) 'The Navy will build tactical cyber teams'. *Fifth Domain*, 6th December. Available at: https://www.fifthdomain.com/dod/navy/2019/12/06/the-navy-will-build-tactical-cyber-teams/ [Accessed: 1st August 2020].

Pomerleau, M. (2019) 'How the Air Force has reorganized its cyber staff'. *Fifth Domain*, 20th September. Available at: https://www.fifthdomain.com/news-

letters/digital-show-daily/2019/09/20/how-the-air-force-has-reorganized-its-cyber-staff/ [Accessed: 1st August 2020].

Pomerleau, M. (2019) 'New authorities mean lots of new missions at Cyber Command'. *Fifth Domain*, 8th May. Available at: https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/ [Accessed: 1st August 2020].

Pomerleau, M. (2018) 'How the Army will infuse cyber operations on the battlefield'. *Fifth Domain*, 5th July. Available at: https://www.fifthdomain.com/dod/army/2018/07/05/how-the-army-will-infuse-cyber-operations-on-the-battlefield/ [Accessed: 1st August 2020].

Poulter, A., Mackay, M. (2018) 'The Internet of Military Things'. Slideshow, 3rd July. Salisbury, Defence Science and Technology Laboratory [DSTL]. Available at: https://www.c-iot.ecs.soton.ac.uk/sites/www.c-iot.ecs.soton.ac.uk/files/AndrewPoulter.pdf [Accessed: 1st August 2020].

Rivers, B. (2020) 'Air Force to Integrate 'Project Maven' AI Scope into ABMS; Will Roper Quoted'. *Executive Gov*, 11th August. Available at: https://www.executivegov.com/2020/08/air-force-to-integrate-project-maven-ai-scope-into-abms-will-roper-quoted/ [Accessed: 10th September 2020].

Rothstein, M. & Saltzman. B. (2019) 'Multi-Domain Operations'. Doolittle Series 18. LeMay Paper 3. Montgomery AL, LeMay Center for Doctrine Development and Education. Available at: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/LP_0003_Multi_Domain_Operations.pdf [Accessed: 1st October 2020].

Royal Air Force. (c.2020) 'Integrated Review Air & Space Proposition'. RAF Astra.

Royal Navy. (2020) 'Royal Navy backs MoD Initiative to see Defence and Industry work Closer'. Press release, 28th February. Available at: https://www.royalnavy.mod.uk/news-and-latest-activity/news/2020/february/28/200228-integrated-warrior [Accessed: 1st August 2020].

Russell, S., Abdelzaher, T. & Niranjan, S. (2019) 'Multi-Domain Effects and the Internet of Battlefield Things'. *MILCOM 2019: 2019 IEEE Military Communications Conference*. 724-730. Available at: https://ieeexplore.ieee.org/document/9020925/ [Accessed: 1st August 2020].

Sabbagh, D. (2020) 'UK to launch specialist cyber force able to target terror groups.' The Guardian, 27th February. Available at: https://www.theguardian.com/technology/2020/feb/27/uk-to-launch-specialist-cyber-force-able-to-target-terror-groups [Accessed: 1st August 2020].

Sanders, P. (2020) 'Commander Strategic Command [...] Speech at the Air and Space Power Conference,' 15th July. Speech transcript. Northwood, UK Strategic Command. Available at: https://www.gov.uk/government/speeches/commander-strategic-command-general-sir-patrick-sanders-speech-at-the-air-and-space-power-conference [Accessed: 1st August 2020].

Schneider, J. (2017) 'Cyber and Crisis Escalation: Insights from Wargaming'. Draft research paper. Newport RI, United States Naval War College. Available at: https://paxsims.files.wordpress.com/2017/01/paper-cyber-and-crisis-escalation-insights-from-wargaming-schneider.pdf [Accessed: 1st August 2020].

Schubert, J., Brynielsson, J., Nilsson, M. & Svnmarck, P. (2018), 'Artificial Intelligence for Decision Support in Command and Control Systems'. *ICCRTS 2018: 23rd International Command and Control Research and Technology Symposium*, November. Available at: https://www.foi.se/download/18.41db-20b3168815026e010/1548412090368/Artificial-intelligence-decision_

FOI-S--5904--SE.pdf [Accessed: 24th November 2020].

Schulze, M. (2020a) Cyber in War: Assessing the Strategic, Tactical and Operational Utility of Military Cyber Operations. In: Jančárková, T., Lindström, L., Signoretti, M., Tolga, I., & Visky G. (eds.) 20/20 Vision: The Next Decade. 12th International Conference on Cyber Conflict. Tallinn, Estonia, NATO Cooperative Cyber Defence Centre of Excellence. Available at: https://ccdcoe.org/uploads/2020/05/CyCon_2020_10_Schulze.pdf [Accessed: 1st September 2020].

Schulze, M. (2020b) 'Militärische Cyber-Operationen: Nutzen, Limitierungen und Lehren für Deutschland'. Stiftung Wissenschaft und Politik. Berlin, SWP-Studie 15, 15th August. Available at: https://www.swp-berlin.org/publikation/militaerische-cyber-operationen/ [Accessed: 16th August 2020].

Schulze M. (2020c). 'German Military Cyber Operations are in a Legal Gray Zone'. *Lawfare*, 8th April. Blog. Available at: https://www.lawfareblog.com/german-military-cyber-operations-are-legal-gray-zone [Accessed: 1st August 2020].

Sengupta, K. (2019) 'Army to form new hybrid-warfare division'. *The Independent*, 1st August. Available at: https://www.independent.co.uk/news/uk/home-news/uk-army-hybrid-warfare-division-conflict-intelligence-cyber-a9030281.html [Accessed: 1st August 2020].

Sfar, A., Natalizio, E., Challal, Y. & Chtourou, Z. (2018) 'A roadmap for security challenges in the Internet of Things'. *Digital Communications and Networks*. 4 (2), 118-137. Available at: https://doi.org/10.1016/j.dcan.2017.04.003 [Accessed: 1st August 2020].

Skinner, D. (1988) 'Airland Battle Doctrine'. Professional Paper 463 September. Alexandria VA, Center for Naval Analyses. Available from: https://apps.dtic.mil/dtic/tr/fulltext/u2/a202888.pdf [Accessed: 1st August 2020].

Smeets, M. (2018) 'Integrating offensive cyber capabilities: meaning, dilemmas and assessment'. *Defence Studies*, 14th August. 18 (4), 395-410. Available at: https://doi.org/10.1080/14702436.2018.1508349 [Accessed: 1st August 2020].

Stafford, N. (2019) 'The Alliance Strikes Back: Using Multi-Domain Operations to Counter Russian Hybrid Warfare in the Baltics'. Master's thesis. Fort Leavenworth KS, United States Army Command and General Staff College. Available at: https://apps.dtic.mil/sti/pdfs/AD1105226.pdf [Accessed: 1st August 2020].

Stover, S. (2020) 'Battalion helping shape Army tactical capabilities in the information environment'. US Army, 30th January. Available at: https://www.army.mil/article/231091/battalion_helping_shape_army_tactical_capabilities_in_the_information_environment [Accessed: 1st August 2020].

Strange, J. & Iron, R. (2004) 'Center of Gravity: What Clausewitz Really Meant'. *Joint Force Quarterly*. 35, 20-27. Available from: https://apps.dtic.mil/dtic/tr/fulltext/u2/a520980.pdf [Accessed: 1st August 2020].

Stronell, A. & Gady, F. (2020) Interviews with former British intelligence official, 14th September – 2nd October.

Taylor, C. & Kay, L. (2019) 'Putting the Enemy between a Rock and a Hard Place: Multi-Domain Operations in Practice'. West Point NY, Modern War Institute at West Point, 27th August. Available from: https://mwi.usma.edu/putting-enemy-rock-hard-place-multi-domain-operations-practice/ [Accessed: 1st August 2020].

The Economist. (2019) 'Artificial intelligence is changing every aspect of war,' 7th September. Available at: https://www.economist.com/science-and-technology/2019/09/07/artificial-intelligence-is-changing-every-aspect-of-war [Accessed: 1st October 2020].

The Telegraph. (2018) 'Britain steps up cyber offensive with new £250m unit to take on Russia and terrorists,' 21st September. Available at: https://www.telegraph.co.uk/news/2018/09/21/britain-steps-cyber-offensive-new-250m-unit-take-russia-terrorists/ [Accessed: 1st August 2020]..

Thompson, E. (2019) 'I2CEWS'. Factsheet, 1st October. Atlanta GA, Defense Visual Information Distribution Service [DVIDS]. Available at: https://www.dvidshub.net/news/353065/i2cews-factsheet [Accessed: 1st August 2020].

Townsend, S. (2019) 'Defining the 'Domain' in Multi-Domain'. *Joint Air and Space Power Conference 2019: Shaping NATO for Multi-Domain Operations of the Future*. 7-12. Available at: https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf [Accessed: 30th September 2020].

Tucker, P. (2020) 'The Air Force's 'Connect Everything' Project Just Had a Big Success'. *Defense One*, 11th September. Available at: https://www.defenseone.com/technology/2020/09/air-forces-connect-everything-project-just-had-big-success/168407/ [Accessed: 12th September 2020].

United States Army War College. (2020) *Strategic Cyberspace Operations Guide*, 1st June. Carlisle PA, Center for Strategic Leadership. Available at: https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf [Accessed: 1st August 2020].

US Army Cyber Command. (2020) 'Cyber Mission Force'. Factsheet, 10th February. Washington DC, Department of Defense. Available at: https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/ [Accessed: 1st August 2020].

US Army Training and Doctrine Command [TRADOC]. (2018) 'The US Army in Multi-Domain Operations 2028'. TRADOC Pamphlet 525-3-1, 6th December. Fort Eustis VA, US Army. Available from: https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf [Accessed: 1st August 2020].

US Army Training and Doctrine Command [TRADOC]. (December 2017) 'Multi-Domain Battle: Evolution of Combined Arms for the 21st Century, 2025-2040'. Version 1.0. Available from: https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf [Accessed: 1st August 2020].

US Cyber Command. (2017) 'USCYBERCOM 120-Day Assessment of Operation GLOWING SYMPHONY: Executive Summary'. Internal report, 12th April. Washington DC, Department of Defense. Available at: https://nsarchive.gwu.edu/dc.html?doc=6655597-National-Security-Archive-6-USCYBERCOM [Accessed: 1st October 2020].

US Cyber Command. (2016). 'USCYBERCOM 30-Day Assessment of Operation GLOWING SYMPHONY: Executive Summary'. Internal report, 13th December. Washington DC, Department of Defense. Available at: https://nsarchive.gwu.edu/dc.html?doc=6655596-National-Security-Archive-5-USCYBERCOM [Accessed: 1st October 2020].

Warrell, H. (2020) 'Covid-19 crisis accelerates UK military's push into virtual war gaming'. *Financial Times*, 19th August. Available at: https://www.ft.com/content/ab767ccf-650e-4afb-9f72-2cc84efa0708 [Accessed: 1st October 2020].

Warfare Today. (2019) 'British Army Launches New 6th Division: Specialist Brigades Group to Deliver Cutting-Edge Capability,' 1st August. Available at: http://www.warfare.today/2019/08/01/british-army-launches-new-6th-division/ [Accessed: 1st August 2020].

Watling, J. & Roper, D. (2019) 'European Allies in US Multi-Domain Operations'. Occasional Paper, October. London, Royal United Services Institute. Available at: https://rusi.org/sites/default/files/20190923_european_allies_in_us_multi-domain_operations_web.pdf [Accessed: 1st August 2020].

PART IV:
Information Sharing, Cyber Threat Intelligence and Exercises

Repairing the Foundation: How Cyber Threat Information Sharing Can Live Up to its Promise and Implications for NATO

Michael Daniel
President & CEO
Cyber Threat Alliance

Joshua Kenway
Cybersecurity Associate
Cyber Threat Alliance

Abstract: Information sharing has become an overused term that provokes eye rolls within the cyber security community. Yet, effective sharing would improve cyber defences. Why has information sharing failed to live up to its promise? The difficulty stems from three faulty assumptions, namely that cyber threat information is primarily technical, that every organisation should produce and consume this technical data, and that sharing such information is easy. These faulty assumptions have resulted in ineffective policy, misaligned incentives, and insufficient information sharing. Instead, four alternative assumptions should drive sharing threat information consisting of multiple complex information types with values that vary across consumers. Relevance and comparative advantage should drive which organisations share what information, as information sharing is challenging and must overcome four barriers and trust is a necessary component of any sharing activity. These alternative assumptions have several implications. Few organisations should share more than three or four sub-types of cyber threat information. Information sharing programmes should focus on the types of information most valuable for their constituents and they need processes and rules that build trust over time. Reducing the number of organisations sharing technical information would make achieving scale and speed easier. The information sharing burden would decrease while the value would go up, increasing the probability of information sharing. Additional standard formats and sharing systems would emerge, with increasing degrees of automation. Finally, effective cyber threat information sharing requires planning, long-term investment, and sustained commitment. Information sharing is not an unsolvable problem. Changing the underlying assumptions will increase the volume, quality, and utility of cyber threat information sharing. In turn, more effective sharing will enable defenders to better understand

adversaries in the context of their organisation, enabling them to develop mechanisms to disrupt adversary activities more strategically and raise the level of cyber security across the digital ecosystem. Only then can information sharing finally live up to its promise.

Keywords: *Information sharing, threat intelligence, cyber security*

1. INTRODUCTION

Information sharing has become such an overused but under-performing concept that the term tends to provoke eye rolls within the cyber security community. Yet, most practitioners and policymakers agree that better information sharing would improve defences against rapidly evolving cyber threats. Virtually every relevant panel, study, or review over the last 20 years has recommended increased information sharing as a key step in improving cyber security. The logical question is why information sharing has not increased. Its lack remains a barrier to better cyber security, whether within NATO or the broader digital ecosystem.

This chapter will identify three faulty assumptions that have prevented cyber threat information sharing from living up to its promise that cyber threat information consists primarily of technical data, that every organisation should consume this technical data, and that information sharing is easy. It then establishes a framework for updating the current approach to information sharing by distinguishing the characteristics and value of different threat information types, using relevance and comparative advantage as the basis for producing and consuming threat intelligence, addressing key barriers to information sharing, and identifying trust as a necessary component of effective information sharing. Finally, the chapter explores the implications of these changed assumptions for more effective information sharing, including within NATO's information sharing ecosystem.

A. Technical Level Cyber Threat Information Sharing in NATO

NATO adopted technical cyber threat information sharing early on through an instance of the open-source Malware Information Sharing Platform (MISP) (NATO, 2013; MISP, 2020a), which the Alliance leverages to privately share information with member states, industry partners, and national Computer Emergency Response Teams (CERT) (Schrooyen, 2017). NATO uses MISP for the exchange of classified technical information with tactical and operational value and information sharing with participating partners is filtered according to its classification level (Schrooyen, 2017). Using MISP only for classified technical information sharing limits its value because it restricts the number of potential partners and excludes other valuable types of strategic and operational information. Over-classification impedes information sharing, something which NATO has acknowledged (NATO, 2012).

NATO also maintains a best practice and threat information sharing relationship with EU-CERT (NATO, 2016) and is building an Industry Cyber Part-

nership (NICP) (NATO, 2020). These two programmes provide NATO with the foundation needed to meet the challenges of information sharing explored in this chapter. Key industry partners include Oracle (NATO, 2019a), RSA Security (NATO, 2017), FireEye (Fireye, 2016), Cisco (NATO, 2016), CY4GATE, Thales, Vodafone (NATO, 2018), BT, Minded Security, Lockheed-Martin, Fortinet, and Symantec (Schrooyen, 2017). The NICP has broad goals, including improvements to the sharing of best practices, expertise, experience, and information 'including [...] on threats and vulnerabilities' (NATO, 2020).

In parallel, the Alliance's efforts to operationalise a Cyber Security Collaboration Hub by 2023 (NATO, 2019b), which will allow member states 'to quickly and securely share information with each other, and with the [Alliance]' (NATO, 2019c), could address some of the challenges raised in this chapter. However, this chapter argues that NATO should shift its approach to information sharing to assume a leadership position in this area.

2. FAULTY ASSUMPTIONS: OVERPROMISING AND UNDERACHIEVING

Underlying the slow progress on information sharing are three faulty underlying assumptions: (1) cyber threat information consists primarily of technical data; (2) every organisation should be producing and consuming technical cyber information; and (3) sharing cyber threat information is easy.[1] These fallacies are implicit, rather than explicit, and so have largely avoided critical review or academic assessment. Further, they have resulted in counter-productive policy, misaligned incentives, and ineffective cyber security. To address these shortcomings, different foundational assumptions are needed. In turn, using better assumptions can make information sharing a more effective tool against cyber threats.

A. Cyber Threat Information Consists Primarily of Technical Data

Within the cyber security community, the term 'information sharing' primarily refers to the exchange of technical data that identifies malicious activity such as malware and malicious domain names. While several scholars (Friedman et al., 2015; Chismon & Ruks, 2015) acknowledge that such exchanges should also include other types of information, the emphasis is on technical data in practice. For example, the main use cases or core functionalities associated, respectively, with the two commonly used cyber information sharing standards, Structured Threat Intelligence eXchange (STIX) and the Malware Information Sharing Platform (MISP), focus on technical

[1] The cybersecurity field has long debated whether to distinguish between 'intelligence' and 'information'. While a distinction between intelligence and information may be important in some contexts, this chapter will set aside that argument and use the term 'information sharing' because it is understood by a broader audience. This approach is further legitimised by documentation from the MITRE Corporation describing its 'de-facto standard for describing threat intelligence' (Sauerwein et al., 2017: p. 838), specifically a white paper on 'Standardizing Cyber Threat Intelligence Information [emphasis added]' (MITRE, 2012).

information (MITRE, 2012; MISP, 2020b). Cyber threat information sharing 'primarily focus[es] on sharing of indicators of compromise' (Sauerwein et al., 2017: p. 838), leading to a situation in which the activities of almost every established sharing platform are 'comparable to data warehousing' (ibid: p. 849). Many US government programmes and existing statutes either explicitly or implicitly focus on this type of information sharing; meanwhile, companies are investing billions of dollars in an effort to consume and analyse technical cyber threat information (Verified Market Research, 2020).[2]

The assumption that cyber threat information is equivalent or primarily composed of technical data severely limits the potential value of information sharing. Technical data, while necessary, is not the only form of information that can provide value. For example, a warning from the US Federal Bureau of Investigation (FBI) that a specific Chinese cyber group is targeting a US company with cyber-enabled theft of intellectual property would be a useful piece of non-technical intelligence for that company. Written advisories about vulnerabilities and associated patches are critical to organisations using vulnerable software or hardware; in fact, such information is far more useful to most organisations than technical data on one of the many variations of the LockerGoGo malware. The most common interpretation of information is too narrow.

B. Every Organisation Should Produce and Consume Technical Data

If the underlying assumption is that information sharing means technical information, then it logically follows that most policies, infrastructure, and programmes for sharing are built around the idea that most organisations should produce and consume technical information. If everyone were to collect, share, and consume such data, the thinking goes, security would improve across the ecosystem. The problem with this logic is that most organisations are lousy at collecting, producing, and consuming technical data—and always will be. Most companies do not have the capability to identify a malware binary, analyse it, and use the resulting information, nor would they know how to handle a malicious domain name. As a practical matter, this situation will not change; no country will have enough cyber security professionals for every organisation to have this capacity. Small and medium businesses do not and will not have the resources to collect, process, share, and consume technical data regularly. This limitation does not mean such organisations would not benefit from cyber threat information sharing; rather they need different information.

Neither is this approach economically efficient. Most organisations do not need access to technical data in real-time. Despite the rapidly changing nature of cyber threats in a technical sense, for most organisations, cyber security requirements and best practices do not change much from day to day.

[2] For example, see the Cybersecurity Information Sharing Act of 2015 (Consolidated Appropriations Act of 2016, Division N, Cybersecurity Information Sharing Act of 2015) and the Automated Indicator Sharing Program (DHS Cybersecurity and Infrastructure Security Agency, 2020).

In addition, not every business has in-house technical accounting or legal skills—why should cyber security be different? Current practice does not sufficiently differentiate between organisations in terms of what information they should share under what circumstances and how frequently.

C. Information Sharing is Easy

In January 2008, the US government started the Comprehensive National Cybersecurity Initiative (CNCI), formalising it in National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 (The White House, 2010). 'Connect the Centers,' one of CNCI's twelve lines of effort, focused on information sharing with the goal of linking the US government's cyber centres into one common operating picture; over the long-term, it was intended to incorporate the private sector. Everyone assumed that this element would be the easiest to implement and the first to be completed. However, thirteen years later, this element is arguably one part of the CNCI vision that remains unrealised as the cyber security centres are not seamlessly connected and many silos remain stubbornly in place.

A similar situation has played out in the private sector with the creation of Information Sharing and Analysis Centers (ISACs). The assumption was that companies would eagerly join these organisations, share what they knew and consume the information shared by others. Yet, more than twenty years after the concept was formalised into national legislation, many sectors are just now forming an ISAC and, even in the most successful of them, the percentage of participants that actively share information is widely understood within the industry to remain low.

Public sector efforts to share information with the private sector have suffered analogous problems. The US government created the Automated Indicator Sharing (AIS) programme as a free service for general businesses, but few organisations have signed up and even fewer contribute to the programme (Marks, 2018). This is unsurprising if we look at what is being shared; a US government report from 2018 suggested that just two or three out of the 11,447 indicators submitted to AIS by the Department of Homeland Security were 'malicious and related to cyber incidents [... while] many of the indicators received were false positives or redundant information' (DHS Office of Inspector General, 2017: p. 15).

The three examples highlight that information sharing is difficult for a variety of reasons. Simply creating programmes and establishing sharing mechanisms is insufficient without addressing obstacles to sharing actionable information. These include underlying factors such as over-classification, reputational risk, and legal concerns, as well as operational hurdles around validation, standardisation, timeliness, and automation (Zibak & Simpson, 2019).

3. REBUILDING INFORMATION SHARING: NEW IMPERATIVES

These incorrect assumptions have undermined information sharing as an effective tool against cyber threats, yet policies, structures, and processes must be based on assumptions about the overall environment in order to function. As a replacement for the faulty assumptions explained above, this chapter proposes four alternative presumptions to enable effective information sharing. First, cyber threat information consists of multiple information types across different levels, with distinct value to different consumers, meaning that information sharing needs to be tailored and nuanced. Second, for this reason, relevance and comparative advantage should drive sharing activities. Third, effective information sharing efforts must overcome context-specific technical, economic, legal, and cultural barriers; and fourth, trust is a necessary component of information sharing. The rest of this section will explore these alternative presumptions in greater detail.

A. Types of Cyber Threat Information

Chismon and Ruks (2015) assembled a useful taxonomy of cyber information categories based on the kind of decisions the information informs. A modified version of their taxonomy is shown in Table I.

Table I: Categories of Cyber Threat Information

Category of Cyber Threat Information	Examples of Information Conveyed	Intended Audience	Decision Example	Timeframe of Use
Technical	Indicators of malicious activity (e.g., malware hashes or IP addresses)	Cyber security vendors and network provider	Should the network security tool allow this packet through?	Immediate
Tactical	Details related to a specific/ impending cyber attack	Network defenders (i.e. relevant staff and decision-makers)	Do we need to change a security setting today?	Short Term
Operational	Malware types; Attacker tactics, tools, and procedures (TTPs)	Senior-level security personnel / managers	How often should we patch our networks?	Medium Term
Strategic	High-level information on changing cyber risk	Executives / senior decision-makers	Should we change our risk calculation because a new adversary is targeting our industry?	Long Term

As detailed in Table I, different categories of information, from technical to strategic, are intended for different consumers. However, information across the four levels—technical, tactical, operational, and strategic—is interrelated. For example, technical and tactical information can be combined to generate operational cyber threat information to improve organisational understanding of an impending attacker's methods and capabilities (Chismon & Ruks, 2015). Similarly, post-incident analysis of technical cyber threat information often provides the foundation for the implementation of a tactical level decision. A holistic assessment of technical, tactical, and operational inputs drives the output of strategic cyber threat information. Despite these complex relationships, this taxonomy provides a useful way to think about cyber threat information and is indicative of why technical data-sharing should not be the sole focus of information sharing programmes. Smaller or less mature organisations are unlikely to find much utility in technical or tactical information sharing, while even larger organisations may miss out on key operational or strategic information insights if they focus exclusively on the technical information. For this reason, the Cyber Threat Alliance (CTA), which includes established cyber security vendors and related enterprises, shares a total of ten types of actionable cyber threat information across these four categories, as recalled by the authors and detailed in Table II.

Table II: Examples of Cyber Threat Information, by Category

Technical Level Information	Tactical Level Information	Operational Level Information	Strategic Level Information
Indicators and Sightings Hashes, binaries, IP addresses, URLs, etc.	**Targeted Warnings** Information that a malicious actor is targeting a specific organisation in the near term	**Vulnerabilities and Exploits** Descriptions of security flaws in software and how bad actors can exploit them	**Best Practices** Methods for organising, securing and maintaining IT networks to prevent, detect, respond and recover from cyber threats or incidents
Context Metainformation about technical indicators, including date and time detected, location of detection, type of organisation targeted, associated actor group	**Situational Awareness** Details of activity happening on a network and / or the broader internet at any given time	**Defensive Measures** Methods to mitigate exploits and counter adversary TTPs	**Strategic Warnings** General information about cyber threats, such as typical targets for an adversary and how they are evolving
Tactics, Techniques and Procedures Methods adversaries can use to carry out malicious activity		**Attribution** Identifying who is responsible for specific malicious activity	

Understanding the value of these various forms of cyber threat information requires taking a more mature and nuanced view than the simplistic assumption that more information sharing means better security. This expanded conceptual framework for cyber threat information sharing reflects the diversity of information that industry leaders already know must be shared to strengthen defences. Each type informs a different aspect of cyber security and has a different value in different situations. Broad adoption of this (still high-level) extension to the framework provided by Chismon and Ruks (2015) would enable cyber security practitioners to develop more nuanced and useful policies for information sharing.

B. Relevance and Comparative Advantage in Information Sharing

In other disciplines, from finance to health to politics to sports, organisations do not produce and consume the same information equally. Instead, wide variation occurs based on relevance to business models, missions, and perceived benefits. Cyber security practitioners and policymakers should expect cyber threat information sharing to behave similarly. Different organisations should produce and consume different types of information based on two principles: relevance and comparative advantage. These two concepts should drive who should be sharing what information with whom, in what detail, and at what periodicity.

1) Relevance of Information

Companies, non-profit organisations, and government agencies all have goals or missions and employ specific business models to achieve those goals. Information sharing should relate directly to an organisation's goals and business model. Thus, a cyber security vendor should share technical cyber threat information at speed and at scale continuously because it is directly relevant to their business model. Conversely, a medium-sized manufacturer primarily needs strategic and operational level cyber threat information—strategic warnings, best practices, and tactical warnings (e.g., if a government learns that the business or its industry is being targeted)—all of which need only to be updated when a change has occurred. Technical cyber threat information provided at scale to this business would simply not be useful.

2) Comparative Advantage of Information Sharing

Even if some organisations can produce certain information types, others might be more efficient at that work. For example, although governments can use their intelligence and law enforcement capabilities to collect, process, and produce technical cyber threat information, they do not have a comparative advantage in that information type. Private sector companies can perform that function just as efficiently. However, governments have a comparative advantage in other categories, such as attribution of cyber attacks, strategic warnings, and tactical warnings, which benefit from nation-state-level intelligence capabilities and authorities. As in other activities, the principle of comparative advantage should determine which organisations should be collecting, processing, sharing, and consuming different types of information.

C. Technical, Economic, Legal and Cultural Barriers

At first glance, the barriers inhibiting information sharing seem quite varied. However, a closer review shows they fall into four categories: technical, economic, legal, and cultural. While their specific manifestations and relative significance will vary across sharing contexts, these barriers can combine in various ways to create a formidable obstacle to sharing.

Technical barriers prevent information from moving rapidly at scale or in easily consumable formats. For example, inconsistent definitions and terminology and difficulty in achieving interoperability and automation remain significant obstacles (Zibak & Simpson, 2019). In turn, these barriers often inhibit the usability or reliability of shared information (ENISA, 2017).

Economic barriers stem from the inability to identify a clear return on investment from sharing activities. Organisations 'participate in sharing networks when their return is more than the cost to participate' (Vázquez et al., 2012: p. 432). This problem can be compounded by first-mover disadvantage, given that 'establishing threat intelligence sharing infrastructure is expensive ... [while] in the long run, intelligence sharing could help bring down the overall security cost' (Zibak & Simpson, 2019: p. 7). Absent a clear and immediate prospect of a return on investment, proponents often have difficulty making the business case to establish, invest in or sustain sharing activities. Legal barriers come from uncertainty about what information can be shared under what circumstances or unanswered questions about liability, fines, or prosecution. These uncertainties deter organisations from sharing. Privacy laws can hinder sharing by inadvertently classifying certain cyber threat information as private and thereby limiting how it can be used or distributed (Panda Security, 2018). These legal concerns require sharing organisations to undertake extensive consideration of their potential implications (Borden et al., 2018; Albakri et al., 2019).

Finally, cultural barriers can also impede sharing (Luiijf & Kernkamp, 2015). For cyber security companies, it can be hard to overcome the idea that retaining unique data yields a competitive advantage. For other organisations, it can be hard to overcome sentiments such as 'no one would target me', 'cyber security is too complex for executives and non-technical employees to understand', or 'falling victim to hackers is inevitable, so why bother?' For governments, long-standing views about the appropriate respective roles of the public and private sectors get in the way of cooperation and sharing.

The good news is that, over the last twenty years, practitioners have developed ways to overcome these barriers. The bad news is that none of these methods is frictionless or cost-free. For example, adopting technical standards for information sharing may require organisations to adjust business processes or infrastructure; high initial costs may need to be met with loans that are paid back by future sharing participants; legal consultations may be needed to shape sharing rules; and reluctant executives may need the benefits of information sharing to be explained in bottom-line terms.

Across the board, information sharing requires organisations to expend resources, either money or time. These costs can decrease but do not disappear. Yet, to be worthwhile, information sharing needs to be sustained and organisations have to pay a long-term, regular cost for engaging in information sharing activities. This requirement, in turn, means that information sharing requires incentives to achieve the scope, scale, and speed required for effective cyber defence. Such incentives can range from the individual (avoiding the costs of a cyber incident) to the public (government grants) to the avoidance of sticks (fines or penalties for not engaging in appropriate sharing). Regardless, information sharing laws, policies, programmes, and structures should assume that information sharing is resource-heavy and requires sustained investment to occur.

D. Trust as a Necessary Component of Information Sharing

Experience from previous initiatives and programmes demonstrates that information sharing only occurs when the providers and recipients have a degree of trust. As noted by Wagner et al. (2018), trust 'plays a critical role in sharing' (p. 5). The European Network Information Agency (ENISA) observes that in situations where trust between members of the community is diminishing or non-existent the value of information shared is undermined (ENISA, 2013). For information sharing to work, it is necessary to 'foster confidence for stakeholders that the provided information will be acted upon as intended' (Wagner et al., 2018: p. 5). Information providers have to understand who will receive their information, what they will do with it, and what level of information sharing-related risk to expect, while information recipients want to know where the information came from and its reliability.

To reach this level of confidence, information sharing organisations should 'provide control mechanisms to specify what information is shared, how much of it and with whom' (Sauerwein et al., 2017: p. 845). According to ENISA (2012, cited by Vázquez et al., 2012: p. 433), the use of intentionally carefully designed trust-building mechanisms, such as 'the policies, membership rules, requirement for security clearance and interaction type' can be beneficial in the context of information sharing and will support the creation of trust.

Absent trust, information sharing will not occur no matter what structures and incentives are put in place. Trust does not require that the participants all like each other, nor does it mean they share everything. Trust means that participants have a reasonable belief that all other participants will adhere to the agreed rules.

4. IMPLICATIONS OF INFORMATION SHARING IMPERATIVES

The new information sharing presumptions proposed in this chapter—careful consideration of information type and relevance, comparative advantage in information production, how to overcome existing context-specific bar-

riers, and how to create and maintain trust—make the cyber threat information sharing landscape far more complex than most people envision. Yet, this very complexity provides an opportunity for simplification: rather than everyone trying to share everything all the time, organisations can concentrate on the information types most relevant to them. Information sharing architectures, policies, and systems should assist organisations in focusing their information sharing activities. Although identifying all the implications is beyond the scope of this chapter, some more prominent ones are worthy of mention.

Few organisations will share every type of cyber threat information. Most organisations should focus on the types of information most relevant to their business model. For example, under this paradigm, only organisations with strong technical capabilities would share technical cyber threat information: cyber security providers, telecommunications companies, Internet Service Providers (ISPs), Managed Security Service Providers (MSSPs), and large, multinational companies in critical industries. Government agencies would focus less on producing stand-alone technical indicators of compromise (IOCs), which industry has in abundance, and more on combining that information with strategic and tactical warning about specific threats, since their comparative advantage lies in their intelligence and law enforcement capabilities. Most citizens, businesses and organisations would primarily consume information about best practices and defensive measures.

The focus of information sharing programmes should change. Since most organisations do not need to produce or consume technical cyber threat information, government cyber security initiatives should reflect this. These programmes should instead encourage most organisations to hire a cyber security vendor or MSSP. Those service providers would consume the technical, contextual, vulnerability, and exploitation information and use it to make security adjustments such as updating blacklists or prioritising patches. Most organisations would primarily consume updates to best practice and strategic or tactical warnings. This change would make information sharing programmes more relevant and cost-effective.

Information sharing programmes need to build trust. Since trust is a key component for effective information sharing, programs, structures, and architectures need to build trust over time. Policies and structures should include operational processes designed to enhance confidence and trust when personal rapport among stakeholders may be lacking, particularly when programs are starting (see Sauerwein et al., 2017; Sillaber et al., 2016; Vázquez et al., 2012; Wagner et al., 2019). For example, CTA's information sharing rules specify the nature and scope of the sharing commitment, how members should handle shared information, and what enforcement mechanisms and penalties will be applied for violating those rules. Such clarity and consistency help new members trust that other members will treat their information properly.

Information sharing products can incorporate more than one information type. Since the different information types are interdependent, any given sharing product can contain more than one type. For example, CTA members share technical indicators and tactical context (and occasionally attribution) through the same automated system and standard format (Cyber Threat Alliance, 2020). A more rigorous conceptual framework for information sharing does not require a rigid division among the information types from a software or process flow perspective.

Reducing the number of organisations expected to share technical information would make achieving speed and scale easier. Abandoning the idea that all organisations everywhere should engage in technical cyber threat information sharing makes overcoming the barriers to technical sharing easier. Under this assumption, the number of organisations with the combination of willingness, relevance, and capability to engage in technical cyber threat sharing decreases to a large but manageable number (Aspen Cybersecurity Group, 2018). At this size, having most of these organisations participating in formal information sharing groups becomes a reasonable goal.

The information sharing burden would decrease while the value would go up, increasing the likelihood that organisations voluntarily participate in such activities. By focusing sharing activities on the most relevant information types, the time and monetary investment for most organisations would decrease. At the same time, the connection between shared information and the organisation's mission or business model would become clearer, thereby increasing its value and making that value easier to assess. The decreased burden and increased value would expand the number of organisations that participate in sharing activities.

Additional standard formats for non-technical information types would emerge, along with systems to share those formats with increasing degrees of automation. On the technical side, several standard formats now facilitate automated information sharing, such as the STIX (MITRE Corporation, 2012) and MITRE's Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) frameworks (MITRE Corporation, 2020). More rigorously dividing cyber threat information into different types would encourage other formats to emerge and organisations to adopt them. Standard formats make consumption of information easier for the recipient. Increased automation would increase speed and scale, making sharing more effective.

Effective cyber threat information sharing requires planning, long-term investment, and sustained commitment. For example, technical cyber threat information sharing is not merely a matter of adopting a technical standard and installing software. It takes engineering and analytic time on an ongoing basis as well as maintenance of the technology and processes. Similarly, consuming cyber security best practices is not a one-time endeavour; organisations must incorporate regular review and implementation into their business processes. Absent a long-term commitment from organisational

leadership, sharing usually withers after an initial burst of enthusiasm. Cyber security should take on the same status as other business enablers, such as accounting, legal affairs, and communications; like these areas, cyber security should be a function that all organisations budget for and sustain over the long-term.

5. CONCLUSION

Cyber threat information sharing has bedevilled the cyber security community for at least two decades. Faulty assumptions have prevented this fundamentally sound concept from achieving its potential. But while information sharing is a tough problem, it is not an insoluble one. If the cyber security community adopts different underlying assumptions for information sharing then the volume, quality, and utility of the exchanged information can increase. In turn, more effective, relevant information sharing will enable defenders to better understand and anticipate adversaries, develop mechanisms to disrupt adversary activities more strategically, and raise the level of cyber security across the digital ecosystem. Under these circumstances, cyber threat information sharing can finally live up to its promise to enable better cyber security for everyone.

For NATO, updating programmes to reflect these revised information sharing assumptions would require significant changes to current operations. First, overcoming the technical, economic, legal, and cultural barriers to sharing relevant, actionable information across member countries and economic sectors will require sustained attention, prioritisation, and funding from NATO's senior leadership. Absent such attention, the barriers will likely prove insurmountable. Second, NATO should build on its existing MISP use to create a more comprehensive system of information sharing that broadens the types of information shared and widens the number of recipients. Third, NATO should consider how to better leverage industry for technical information, while enriching that information with government-derived information about context, attribution, and intent. If NATO shifted its approach to information sharing as suggested, the Alliance would have the opportunity to assume a leadership position in this area. If not, NATO will continue to struggle to make information sharing live up to its promise.

6. REFERENCES

Albakri, A., Boiten, E. and De Lemos, R. (2019) Sharing Cyber Threat Intelligence Under the General Data Protection Regulation. *Annual Privacy Forum 2019*, pp. 29-40.

Aspen Cybersecurity Group. (2018) An Operational Collaboration Framework for Cybersecurity. *The Aspen Institute*. Available from: https://www.aspen-institute.org/publications/an-operational-collaboration-framework/ [Accessed 23rd September 2020].

Borden, R.M., Mooney, J.A., Taylor, M. and Sharkey M. (2018) Threat Information Sharing and GDPR: A Lawful Activity that protects Personal Data. *White and Williams LLP, Osborne Clarke LLP and FS-ISAC*. Available from: https://

www.fsisac.com/hubfs/5442200/Resources/FS-ISAC_Threat_Information_Sharing_and_GDPR.pdf [Accessed 23rd September 2020].

Chismon, D. & Ruks, M. (2015) Threat Intelligence: Collecting, Analysing, Evaluating. *MWR Infosecurity & CERT-UK*. Available from: https://scadahacker.com/library/Documents/Best_Practices/CPNI%20-%20Threat%20Intelligence%20-%20Collecting%20Analysing%20Evaluating.pdf [Accessed October 29th 2020].

Cyber Threat Alliance. (2020) *What is the Cyber Threat Alliance?* Available from: https://www.cyberthreatalliance.org/resources/what-is-cta/ [Accessed 23rd September 2020].

DHS Cybersecurity and Infrastructure Security Agency. (2020) *Automated Indicator Sharing (AIS)*. Available from: https://www.cisa.gov/automated-indicator-sharing-ais/ [Accessed 23rd September 2020].

DHS Office of Inspector General. (2017) Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015. *US Department of Homeland Security.* OIG-18-10. Available from: https://www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-10-Nov17_0.pdf [Accessed 23rd September 2020].

ENISA. (2012) Cooperative Models for Effective Public Private Partnerships Desktop Research Report. *European Union Agency for Network and Information Security (ENISA).* Available from: https://www.enisa.europa.eu/publications/copy_of_desktop-reserach-on-public-private-partnerships/ [Accessed 23rd September 2020].

ENISA. (2013) Detect, SHARE, Protect: Solutions for Improving Threat Data Exchange among CERTs. *European Union Agency for Network and Information Security (ENISA)*. Available from: https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs/ [Accessed 23rd September 2020].

ENISA. (2017) Exploring the opportunities and limitations of current Threat Intelligence Platforms (Version 1.0). *European Union Agency for Network and Information Security (ENISA)*. Available from: https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms [Accessed 23rd September 2020].

Fireye. (2016) *NATO and FireEye Announce Cyber Information Sharing Agreement.* Available from: https://investors.fireeye.com/news-releases/news-release-details/nato-and-fireeye-announce-cyber-information-sharing-agreement/ [Accessed 23rd September 2020].

Friedman, J., Bouchard, M., Watters, J., Couch, J. and Hartley, M. (2015) Definitive GuideTM to Cyber Threat Intelligence. *iSight Partners & CyberEdge Group, LLC.* Available from: https://cyber-edge.com/wp-content/uploads/2016/08/Definitive-Guide-to-CTI.pdf

Luiijf, E. & Kernkamp, A. (2015) Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach. Den Haag.

Marks, J. (2018) The government's big idea to bolster the nation's collective cyber defense isn't attracting private-sector participants. *Nextgov*. Available from: https://www.nextgov.com/cybersecurity/2018/06/only-6-non-federal-groups-share-cyber-threat-info-homeland-security/149343/ [Accessed 23rd September 2020].

MISP. (2020a) *Software and Tools*. Available from: https://www.misp-project.org/tools/ [Accessed 23rd September 2020].

MISP. (2020b) MISP (Version 2.4, Readme. md). *GitHub*. Available from: https://github.com/MISP/MISP [Accessed 23rd September 2020].

MITRE Corporation. (2020) Adversarial Tactics, Techniques, and Common Knowledge (ATT&CKTM). Available from: https://attack.mitre.org/ [Accessed 23rd September 2020].

MITRE Corporation. (2012) *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)*. Available from: https://www.mitre.org/sites/default/files/publications/stix.pdf [Accessed 23rd September 2020].

NATO. (2012) Information Sharing with Non-NATO Entities. *Joint Analysis & Lessons Learned Centre*. Available from: http://www.jallc.nato.int/products/docs/factsheet_info_sharing.pdf [Accessed 17th October 2020].

NATO. (2013) *Sharing malware information to defeat cyber attacks*. Available from: https://www.nato.int/cps/en/natolive/news_105485.htm [Accessed 23rd September 2020].

NATO. (2016) NATO expands cyber partnership with Industry. *NATO Communications and Information Agency*. Available from: https://www.ncia.nato.int/about-us/newsroom/nato-expands-cyber-partnership-with-industry.html [Accessed 23rd September 2020].

NATO. (2017) NATO welcomes RSA to its cyber coalition. *NATO Communications and Information Agency*. Available from: https://www.ncia.nato.int/about-us/newsroom/nato-welcomes-rsa-to-its-cyber-coalition.html [Accessed 23rd September 2020].

NATO. (2018) New NATO-Industry cyber partnerships signed at NITEC18. *NATO Communications and Information Agency*. Available from: https://www.ncia.nato.int/about-us/newsroom/new-natoindustry-cyber-partnerships-signed-at-nitec18.html [Accessed 23rd September 2020].

NATO. (2019a) NATO Agency, Oracle sign cyber information sharing agreement. *NATO Communications and Information Agency*. Available from: https://www.ncia.nato.int/about-us/newsroom/nato-agency--oracle-sign-cyber-information-sharing-agreement-.html [Accessed September 23rd 2020].

NATO. (2019b) *Factsheet: NATO Cyber Defence*. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf [Accessed 23rd September 2020].

NATO. (2019c) New NATO hub will gather the Alliance's cyber defenders. *NATO Communications and Information Agency*. Available from: https://www.ncia.nato.int/about-us/newsroom/new-nato-hub-will-gather-the-alliances-cyber-defenders.html/ [Accessed 23rd September 2020].

NATO. (2020) Our Objectives and Principles. *NATO Industry Cyber Partnership*. Available from: https://nicp.nato.int/objectives-and-principles/index.html [Accessed 23rd September 2020].

Panda Security. (2018) *What will happen with WHOIS when GDPR is implemented?* Available from: https://www.pandasecurity.com/mediacenter/security/whois-protocol-gdpr/ [Accessed 23rd September 2020].

Sauerwein, C., Sillaber, C., Mussmann, A. and Breu, R. (2017) Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. In: Leimeister, J.M. and Brenner, W. (Eds.): *Proceedings of the 13th International Conference on Wirtschaftsinformatik, WI 2012, 12-15 February 2017, St. Gallen, Switzerland*, pp. 837-851.

Schrooyen, J. (2017) MISP Usage in NATO. *NATO Communications and Information*

Agency / NATO Computer Incident Response Capability. Available from: https://academiamilitar.pt/images/site_images/Eventos/3rd_Conference/Day_1/MISP_usage_in_NATO_-_Johan_Schrooven.pdf [Accessed 23rd September 2020].

Sillaber, C., Sauerwein, C., Mussmann, A. and Breu, R. (2016) Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. In: *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, WISCS 2016, October 2016, Vienna, Austria.* New York, Association for Computing Machinery, pp. 65–70.

U.S. Congress. (2016) *Consolidated Appropriations Act of 2016, Division N, Cybersecurity Information Sharing Act of 2015*. Available from: https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf [Accessed 23rd September 2020].

Vázquez, D.F., Acosta, O.P, Spirito, C., Brown, S. and Reid, E. (2012) Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships. In: Czosseck, C., Ottis, R. and Ziolkowski K. (eds.) *2012 4th International Conference on Cyber Conflict, CYCON 2012, 5-8 June 2012, Tallinn, Estonia*. Tallinn, NATO CCD COE Publications, pp. 429-445.

Verified Market Research. (2020) Threat Intelligence Market by Deployment Model (Cloud-Based, On-Premise), by Component (Solution, Service), by Organization Size (SMEs, Large Enterprises), by Vertical, Geography and Forecast. Available from: https://www.verifiedmarketresearch.com/product/global-threat-intelligence-market-size-and-forecast-to-2025/

Wagner, T.D., Palomar, E., Mahbub, K. and Abdallah, A.E. (2018) A Novel Trust Taxonomy for Shared Cyber Threat Intelligence. *Security and Communication Networks*. 2018.

Wagner, T.D., Mahbub, K., Palomar, E. and Abdallah, A.E. (2019) Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*. 87 (November 2019). Cairo, Egypt, Hindawi.

The White House. (2010) *The Comprehensive National Cybersecurity Initiative*. Available from: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative [Accessed 23rd September 2020].

Zibak, A. & Simpson, A. (2019) Cyber Threat Information Sharing: Perceived Benefits and Barriers. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES 2019, August 26-29, 2019, Canterbury, United Kingdom. New York, ACM.

Considerations for NATO in Reconciling Challenges to Shared Cyber Threat Intelligence: A study of Japan, the US and the UK

Chon Abraham
Associate Professor of Management Information Systems
William & Mary

Sally Daultrey
Chief Intelligence Analyst
Adenium Group

Abstract: Efforts for developing approaches to exchange information on security incidents, known as Cyber Threat Intelligence (CTI) sharing, are an international imperative for global cyber defence. Japan, the US and the UK are the predominant allied entities in defence of maritime operations for global supply chains in the Asia-Pacific region. These states share common adversaries in cyberspace that work to weaken defences that NATO countries and partners seek to sustain. This chapter explores the challenges and enablers for more effective CTI sharing between Japan, the US and the UK. This chapter offers insights for other non-NATO partners in collectively addressing the global menace of malicious cyber operations, strategic campaigns, and collateral damage on shared networks, infrastructure and missions.

Keywords: *Cyber threat intelligence, cyber security governance, information sharing*

1. INTRODUCTION

Cyber threats are fundamentally changing the nature of warfare and the digital economy with implications for international collaboration and security cooperation (NATO, 2019). Governments and the leadership of multinational companies must understand threat vectors and threat actors to activate their collective response, both in peacetime and during targeted cyber operations. Efforts for developing approaches to exchange information on security incidents, known as Cyber Threat Intelligence (CTI) sharing, is an international imperative (Menges et al., 2019) and governments can no longer rely on voluntary compliance across business ecosystems and supply chains to operationalise international cyber defence. Cyber operations are

increasingly understood as linked to strategic campaigns, particularly when initiated by adversarial countries seeking to shift the relative balance of power amongst targeted countries with rippling global effects (Harknett and Smeets, 2020; NATO CCDCOE, 2017). CTI sharing is therefore essential for all directly and indirectly targeted societies and countries to build a collective understanding of these cyber operations and strategic campaigns in terms of: (1) their true nature; (2) the global reach of effects; (3) the duration; and (4) the extent of data exfiltration and aggregation compromising national security. The sophistication and proliferation of cyber threats are outpacing the capacities of countries to respond using conventional decision structures, to be replaced by dynamic bilateral and regional collaboration architectures. CTI sharing is vital to protecting the global business ecosystem and shared security interests, yet not all nations have comparable capabilities to effectively share and act on threat information.

Japan is NATO's longest-standing partner outside the Euro-Atlantic area and is particularly important to NATO's Asia-Pacific maritime operations (NATO, 2020). Understanding Japan's threat intelligence capabilities and challenges will help in understanding the capabilities of NATO allies like the United States (US) and United Kingdom (UK) in their roles as regular and established partners in maritime operations and trade relations. This chapter explores how more effective CTI sharing between Japan, the US and UK could be promoted, offering insights, which may serve other non-NATO partners in collectively addressing the global menace of malicious cyber operations, strategic campaigns and collateral damage on shared networks, infrastructure and missions.

As part of a larger research project sponsored by the Abe Fellow Program, we conducted 80 interviews over two years with government and private-sector personnel across Japan, the US and UK.[1] We also attended conferences and reviewed the literature on CTI sharing between and among the three countries, strategic culture, cyber risks to critical infrastructure and cyber corporate espionage.[2] In this analysis, we present one facet of the cooperation challenge—understanding the challenges to CTI–which our

[1] Data collection lasted over a two-year period from 2017 to 2019, consisting of insights gather from literature and interviews held face-to-face in-country or virtually that ranged 15 minutes to an hour using open-ended questions or allowing interviewees to provide narratives on the topic. Some insight was gathered from question and answer periods at conferences, meetings or other discussions. When permitted, sessions were recorded, translated, and transcribed. Thematic patterns were analysed in the data relevant to the challenges to CTI from technological, legal, or strategic cultural constraints that impeded seamless transfer of information across nations. Perspectives were sought from respective national cyber authorities, political leaders involved in cyber strategy development, private sector cyber security consultants to these national cyber entities and academic researchers involved in developing national capabilities for CTI. Interviews were conducted by Chon Abraham and Sally Daultrey. When a person who was interviewed required anonymity, in-text references omit interviewee's name. Information was obtained also by personal communication of the authors.

[2] See Appendix I for a summary of research methods.

research to date suggests is the most urgent task and greatest challenge in operationalising international collaboration. It is not enough to know that CTI can be supplied; partners need to know that information will be acted on when received. To reach this level of confidence requires, among other factors, understanding of CTI capabilities within the 'receiver' partner and an appreciation of strategic culture among those involved in the ecosystem of decision, action and accountability.

This chapter presents background literature augmented by insights from the interviews on collective responses and challenges for CTI. We then provide considerations for NATO partners and allies and offer concluding remarks that may guide future research on international CTI sharing.

2. CYBER THREAT INTELLIGENCE SHARING: RESEARCH CONTEXT, INSIGHTS AND CHALLENGES

The WannaCry and NotPetya incidents of 2017, the effects of which can still be seen today, focused government attention on the scale of vulnerabilities in shared global supply chains and civilian infrastructure, particularly in cargo terminals and healthcare services. In May 2018, the European Parliament concluded that these events 'represent breaches of international law by, respectively, the Russian Federation and North Korea, and that the two countries should face commensurate and appropriate responses from the EU and NATO' (European Parliament, 2018). Calls for an international response (NATO CCDCOE, 2017) to the menace of global cyber threats placed cyberspace among the top five global risk domains for 2018 and 2019 (Economist Intelligence Unit, 2019; 2018). Cyber operations are increasingly understood as features of global campaigns (Harknett and Smeets, 2020; Smeets and Lin, 2019) and understanding the extent, tactics and timescale of these campaigns will benefit all who rely on cyberspace and can be significantly improved and accelerated if governments and multinational companies share CTI (114th US Congress, 2015). For example, the Japan-US Defence Cooperation guidelines have included cyberspace since 2015, stating that both governments will cooperate to protect critical infrastructure (Lewis, 2015). In the event of a cyber attack against any part of Japan's critical infrastructure, which is also used by the US Armed Forces and Japan Self-Defence Forces (JSDF), Japan will have the primary responsibility to respond with support from the US (Kyodo, 2019). This could escalate to the US conducting offensive operations on behalf of Japan, raising the stakes for both countries in their response to malicious cyber actors.

The lack of balanced capabilities for CTI fuels risks for vulnerabilities in collective responses for thwarting cyber attacks. For example, the 2013 framework of the US-Japan Defence Cooperation included an Information Security Agreement that allows for the exchange of classified information (US DOD, 2015; MOFA, 2005). However, according to interviewed cyber authorities, Japan still lacks direct access to a shared platform that can deliver forensic data for rapid attribution of cyber attacks. The imperative to address

cyber security risk across national economies, legacy infrastructures and the defence industrial base is today recognised as a priority for national security strategy (Afina et al., 2020; Dunn Cavelty et al., 2019) and a fundamental activity of corporate governance in the digital age (Schinagl and Shahim, 2020). Cyber security has evolved from an enterprise wholly owned by information technology (IT) specialists (von Solms and von Solms, 2018; Naughton, 2016; von Solms and van Niekerk, 2013; Stevens, 2012; Hansen and Nissenbaum, 2009) to a whole-nation challenge that requires active collaboration, set against the human challenges of organisational change, governance and strategic culture. We explore how these challenges have affected the capacity for Japan to share and act on threat intelligence and build effective cyber defence collaboration with the UK and the US that may have implications for other partner and allied NATO countries.

3. CHALLENGES TO SHARING CYBER THREAT INTELLIGENCE

Countries vary in their definition of cyber security but nearly all have drafted some form of cyber security strategy[3] within the past decade, with national cyber security strategies typically developing as part of a coordinated review of national security strategy (Baezner and Cordey, 2019; Luiijf et al., 2013). NATO allies broadly agree on the need to increase cyber resilience, build capabilities including in information sharing and facilitate international collaboration (Ablon et al., 2019; Pernik, 2014), while the imperative for CTI sharing as an organisational capability rather than a data-set is widely recognised in the professional global cyber security community (Wagner et al., 2019). Research in the past decade has begun to compare national cyber strategies for evidence of governance modes (Shackelford and Kastelic, 2015; Weiss and Jankauskas, 2019), harmonisation (Kolini and Janczewski, 2017; Štitilis et al., 2017) and membership of international organisations (Kolini and Janczewski, 2017). Limiting factors and barriers to cooperation in global cyber defence that we have identified include: (i) the capacity and willingness to share threat intelligence; (ii) fuzzy boundaries of responsibility and accountability; and (iii) incomplete or inaccurate understanding of partners' expectations and strategic culture.

A. Challenge One: Capacity and Willingness to Share Threat Intelligence

The US and Japan identified barriers to rapid information-sharing as a particularly complex operational challenge in activating international cooperation for CTI. Incompatible platforms, legal and jurisdictional constraints and conflicting or incompatible strategic cultures were all described as limiting factors. These issues have similarly been identified in studies of CTI-sharing among companies (Wagner et al., 2019; Menges et al., 2019; Koepke, 2017) and for NATO, where inter-organisational trust, incompatible platforms and time-lag in sharing information are among the seven challenges which limit NATO's capacity to work seamlessly with multiple partners (Tolga, 2019). NATO currently uses the Malware

[3] See the NATO CCDCOE library for an index of national cyber strategies (NATO CCDCOE, 2020).

Information Sharing Project (MISP) and launched a Cyber Security Collaboration Network in February 2019 (Pernik, 2014).[4] Japan has formal collaboration agreements with the US and U amongst others, but technical ability for day-to-day collaboration is limited as Japan does not have an interoperable, point-to-point threat intelligence platform allowing direct receipt of data. This is particularly problematic for classified data associated with CTI. Accepted CTI protocols within the threat intelligence community include Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII). These are standards that the US-CERT Automated Indicator Sharing (AIS) capability uses for CTI in the private sector. While senior cyber security researchers and personnel within Japan's cyber authorities have not explicitly noted the use of NATO's adopted MISP, they have observed that some Japanese agencies use STIX as a standard and AIS to share some CTI with US-CERT. However, there is not consistent use across all agencies and in private-public engagements.

We contextualise our analysis of national posture and strategy based on the premise that 'we need to get better at sharing what we know, faster'. The requirement for human interpretation of threat information means that automated CTI is not a fix-all (Wagner et al., 2019) and so the ideal—cyber defence at network speed—is likely to remain an unrealised goal in international cooperative cyber defence until collaboration architectures are stabilised on a foundation of inter-organisational and cross-cultural trust and standardised CTI terminology. Nations need the ability to see a threat and then talk about it on equal terms and this needs direct connectivity for timely response and attribution. According to intelligence personnel that were interviewed in the US, Japan is not getting the full picture fast enough, particularly for classified information that involves CTI (Abraham's interviews and pers. comm., 2019 2 December). This is in part because Japan's cyber personnel in, for example, the Ministry of Defence (MOD), connect with their international peers via proxies, sometimes in allied countries. The process requires de-aggregation and declassification of data for transit and then reassembling when received into classified information sources.

Our interviews also noted a lack of the skill and acumen necessary to understand how to synthesise multi-source threat intelligence in Japan's self-defence forces (JSDF) and other public cyber authorities (Abraham's interviews and pers. comm.,18 December 2019). While the MOD does have something that resembles a cyber-focused speciality akin to those of the US and UK, JSDF cyber personnel are sanctioned to only protect MOD critical infrastructure, even if cyber attacks are detrimental to the Japanese government or society as a whole (Gady and Koshino, 2020). Article 76 of the Self-Defense Forces Act does not define cyber attacks as armed attacks allowing the use of JSDF (Gady and Koshino, 2020; Kono, 2015).[5] This has implications for how the JSDF can cooperate domestically to build cyber acumen in the public and private sectors

[4] See more information provided by the NATO Communications and Information Agency and the MISP (NCIA, 2018; MISP, 2020.)

[5] For a detailed discussion of how cyber attacks are defined in Japanese law, see (Kono, 2015).

and internationally, such as participating in joint cyber offensive training. Deep learning, particularly regarding threat hunting, forecasting intrusion methods, collecting and analysing signal intelligence and forensics on cyber data and networks to determine attribution, are skills needed in Japan's cyber workforce (Abe, 2020). For example, the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) is designated as Japan's cyber coordinating authority, yet operates under a constrained budget and does not have equal legal authority with other agencies and ministries. This reduces its effectiveness and workforce development as it relies on personnel assigned from other Japanese government agencies or the private sector (with or without cyber background), who are rotated in and out of the organisation. The NISC is also constrained in its ability to enforce cyber policy, which is currently fragmented across various ministries. This further limits its ability to influence how Japan's cyber workforce is developed, maintained and provisioned to access and use CTI and related data of various security classifications.

Another practical and major constraint to effective collaboration is Japan's lack of a comparable personnel security clearance system and management programme to ensure classified data is properly handled. Partners need to know that shared intelligence is used and handled safely. These problems are compounded by ambiguity in its classified data ontology to appropriately tag data in compliance with other NATO member countries and partners. There is a disparity in how Japan classifies threat intelligence data in comparison to the US and UK, but consistency is required for nations to be responsive in assessing the effects of threats and their analysis and in timely attribution. According to our interviews, this is also the basis for the difficulty in sharing CTI internally across government and cyber agencies and the private sector. (Abraham's interviews and pers. comm., 2019 4 March, 2 December, 18 December).

While Information Sharing and Analysis Centres (ISACs) are increasingly being used across critical national infrastructure (CNI) sectors in Japan to more quickly readily threat warnings, alerts of malicious activities and threat mitigation data, the detailed classified data required for attribution is often delayed, sometimes by days. US Department of Defense (US DOD) and Japan's Ministry of Defense are exploring options for resolving this issue that are primarily military-to-military, and collaborative exercises for enhancing joint cyber operations and threat intelligence sharing with public entities in the Ministry's cyber task forces and vendors in CNI sectors. The Cybersecurity and Infrastructure Security Agency (CISA) is advising Japan on how to organise an approach around identifying critical national functions that can home in on critical threats to investigate and more effectively coordinate responses. However, this again requires a platform for domestic information exchange. Japan recognises the requirement to be more accountable as a partner to NATO member countries and is actively taking steps to address deficiencies in its capacity to cooperate with others. On 14 August 2020, Defence Minister Taro Kono announced that Japan would seek to expand links with the Five Eyes intelligence-sharing alliance, as

this would allow Japan to obtain classified information at an earlier stage in threat assessment and response (Abe and Rieko, 2020).

As Japan considers the use of offensive cyber capabilities, alliances with NATO and other partners will need a minimum understanding of what tools and weapons have been validated and transparency about at least the function of these cyber assets. Cataloguing and evaluating capacities and cyber assets across countries will help with rapidly mobilising threat intelligence sharing efforts in joint cyber efforts and allowing ease of universal deployment of security standards and vetted state-of-the-art tools. Japan also needs increased capability in assessing how secure the infrastructure is for data transmission and what Japan is equipped to do in terms of technology and personnel skills in the event of a cyber incident at national or international level. According to sources interviewed for this research, a model for assessing this maturity employed by the US Office of the Director of National Intelligence (ODNI) and US Department of Defense is being proposed to the Government of Japan (Abraham's interviews and pers. comm., 6 June 2019).

Limited capacity to absorb and act on CTI compounded by differences in classification and uncertainty over how CTI may be shared, creates a barrier to building trust among partner nations. Continuously improving collective ability to provide threat intelligence and act on it will build capacity to achieve attribution in a timescale that is meaningful for defence and prosecution. This can only be achieved through a whole-of-nation approach.

B. Challenge Two: Boundaries of Responsibility and Accountability

Much of the global attack surface is owned and controlled by the private sector (Ablon et al., 2019; Baezner and Cordey, 2019; Abraham's interviews and pers. comm., 2019 6 June, 8 August, 10 December). Therefore, national cyber security by definition requires cooperation by government organisations with the private sector, within and across national boundaries. Most malicious cyber activity, whether it is cybercrime or potentially of national security importance, happens on privately owned networks. Those private networks are typically not transparent to government cyber authorities in NATO countries. The US, UK and Japan have mechanisms for the private sector to engage and share information, but the robustness of this capacity differs, as does the trust level between the private and public sectors that threatens cyber authorities' ability to receive timely information or to provide assistance. While there are technologies to assist policing entities to determine malicious cyber activity when personal devices such as smartphones are involved (Weaver, 2020; Chesney, 2017), permission for authorities to access private organisational networks is a different matter.

In the opinion of personnel interviewed in the US and UK, the ideal solution for gathering and building CTI for sharing and attribution post-intrusion is to have proper weblogs and backups (Abraham and Daultrey's interviews and pers. comm., 2019 14 July and 9 August; R. Wainwright, 2018, conference and pers. comm, 12 December). With weblogs, authorities can conduct full forensic analysis which allows law enforcement to conduct two primary

functions: use their legal authority and powers to obtain data from other media beyond the initial victim such as infrastructure platform service providers and collate victim web log information with other data points obtained through legal authorities to reconstruct the intrusion and learn about the adversary's tactics. Law enforcement personnel in Japan, the US and UK note that it can be difficult to obtain permission to access private networks, even if there is a suspicion of malicious cyber activity by the private-sector victim organisation (NEC, 2017). In Japan, companies are even less likely to invite government cyber authorities in to aid in determining facts of the intrusion, data exfiltration and insights for remediation. This is due to fear of reputational harm if it is revealed publicly that the company has suffered a cyber attack and was thus not a good steward of its customers' data. CTI is thus limited by transparency and trust within the private sector (NEC, 2017).

Incentivising and activating the private sector to participate in national cyber defence and be held accountable by incorporating robust threat intelligence capabilities into cyber security practice was identified by all interviewees as both a problem and an opportunity (Abraham and Daultrey's interviews and pers. comm., 2019 14 July and 9 August; R. Toth, 2019, pers. comm., 2019 21 July; M. Tsuchiya, M. McConnell, M. Chida, M. Otaka, 2018, conference and pers. comm., 2019 12 December). Companies in Japan have been slow to adapt: only about half conduct cyber security risk assessments that would include their capability to receive and digest threat intelligence data, compared with about 80 per cent in the US and 65 per cent in Europe (Matsubara, 2018b). The lack of cyber leadership in Japanese companies may account for this deficit, as only 27 per cent employ a Chief Information Security Officer (Matsubara, 2018b). Applying risk management standards such as using the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and creating trusted vendor pools of non-blacklisted entities, especially for the defence industrial base, that are also required to share and act on threat intelligence, can all contribute to building a robust threat-sharing public/private ecosystem (Feldman and Witte, 2017).

However, in Japan, cyber and police officials note reluctance by government to receive and relay information to the private sector regarding companies or any entity blacklisted in other nations for dubious behaviour in cyberspace, such as those on the US Department of Treasury Office of Foreign Assets Control (OFAC) list that operationalises cyber protections in the US Foreign Investment Risk Review Modernisation Act. This reluctance stems from fear of both disadvantaging a company if that intelligence is not valid, or infringing its autonomy to manage its internal business processes. This promotes a lack of transparency for cyber events of national security interest and loss of potentially vital threat intelligence data—some of which may date back many years—by Japanese defence contractors. The problem is exacerbated beyond Japan because these contractors also supply other nations, including the US, UK and other NATO countries. In Japan, there is typically no naming, shaming or fines for companies that do not act on threat intelligence even when shared, which contributes to a frail CTI-sharing domestic culture. This

difference in business culture around threat perception and handling may have international implications, particularly for NATO. The Japanese House of Councillors is pushing for legislation requiring Japanese companies to disclose their cyber security postures on their financial statements, which would include their ability to process threat intelligence data. Other countries, including the US and UK, might consider this to encourage CTI capability adoption and cyber resiliency. Japanese companies' corporate taxes are reduced if they can prove that their IT investments include cyber security measures, including CTI processing infrastructure and the promotion of this capability for the shared benefit of the domestic public and private sectors and international stakeholders (M. Tsuchiya, 2019, pers. comm., 6 December; M. DePalo, 2019, pers. comm, 5 March; Matsubara, 2018a).

Globally accessible technologies employed by the private sector complicate CTI assessment for authorities. For example, global virtual private server (VPS) infrastructure can be leased by any private or public entity if allowed in the country. Hostile actors use this medium in cyber attacks, leasing VPSs for short periods, or weaponise leased media by other private sector entities. For law enforcement, getting access to data on VPSs is difficult if the data is in other countries. If the infrastructure is domestic, at least in the US there is a legal process for acquiring it. The Federal Bureau of Investigation (FBI) and Department of Justice (DOJ) have a legal process for gathering information via telecoms devices in the Communications Assistance for Law Enforcement Act (CALEA). However, VPSs are not yet regulated to enable threat intelligence for law enforcement; similarly, no such legislation yet exists in Japan or the UK. Here may be a role for NATO, as a non-state entity, to encourage collaboration for agreements instead of laws across international boundaries to enable threat intelligence gathering and sharing.

Adoption of robust threat intelligence practice and investment in capabilities is not internationally comparable. By 2018, most countries had enacted some form of cyber security legislation, but laws and sanctions are of limited effect against adversaries that do not recognise them (Intelligence and Security Committee of Parliament, 2020; Clarke and Knake, 2020; Stevens, 2012; Tsuchiya, 2019) in jurisdictions where the ability to enforce them is weak and attribution–which relies on threat intelligence – and prosecutions take months or years. A full comparative analysis of the legal basis for cooperation is outside the scope of this chapter, but we note that countries are limited by their own constitution, laws and agreements and the technical capacity to exercise authority within the boundaries of the law (Kono, 2015). For example, the JSDF is planning to develop offensive cyber capabilities that will require revisions to Japan's Self-Defence Forces Law to clarify actions that constitute retaliatory offensive actions (Gady and Koshino, 2020). This requires attribution and sophisticated threat analysis capabilities.

Organising and regulating collective cyber defence presents challenges for many governments and can thwart robust threat intelligence. While the concept of sovereign state security is fairly stable (Hansen and Nissenbaum, 2009), cyberspace uniquely challenges how sovereign countries organise

and project political authority (Weiss and Jankauskas, 2019). In non-authoritarian regimes such as those of NATO allies and partner countries, the role of the state as a security guarantor, legislator, regulator and security partner is challenged by the realities of delivering cyber defence (Dunn Cavelty et al., 2019). Boundaries of responsibility (and thus accountability) are unclear (Stevens, 2012). This problem is illustrated sharply in the case of CNI, given that militaries typically rely partly on national infrastructure owned and operated by private sector organisations. The task of securing CNI from cyber attack has gained attention by governments in articulating their cyber security strategy, particularly after the cyber attacks on Ukraine's electricity grid in December of 2015 and 2016. The demarcation of cyber risk responsibility between utility owner and state is problematic and far from uniform. For example, Japan sees an equal division of labour between government and the private sector (Government of Japan, 2017), while the UK prefers that the private sector assumes responsibility. Coercion by threat actors using CNI and supply-chain vulnerabilities tests the capabilities of countries to respond. Cyber infiltration by adversaries operating within or for other countries seeking to gain intellectual property from US and Japanese defence contractors operating in the Asia Pacific over private networks illustrates the intertwined threats and potential collateral damage of allied and partner countries (MOD, 2018; Lewis, 2015; Tabuchi, 2011). In securing supply chains and shared networks, countries should require accountability by all parties to safeguard and share threat information to avoid proliferating effects.

Assigning responsibility and accountability implies structures and laws. Yet in cyber, analysis of roles and hierarchical structures is only the starting point for identifying barriers to cooperation in an apparently unified global threat landscape (Kuerbis and Badiei, 2017). In creating structures and governance tools, non-authoritarian governments in free-market economies face a challenge and a choice: to develop a single agency that 'owns' cyber on behalf of the nation (and supply a talent base to support it) or require all actors to adhere to laws and standards. The challenge with the first method is to develop a sustainable model that has the endorsement of the private sector while reconciling different organisational cultures (Hannigan, 2019). The second requires devising incentives and fines that are enforceable and adequate to the scale of the task. In a study of 100 cyber strategies and policies, Weiss and Jankauskas (2019) identified two governance modes: delegation and orchestration. When responding to threats, governments tend to delegate authority while maintaining hierarchical control, while in risk mitigation, governments use and orchestrate intermediaries. Overall, we recognise the delegation model in the UK, orchestration in Japan and a hybrid of the two in the US. Interviews for this research suggest that, in the case of the Japan Computer Emergency Response Team (JPCERT), currently a quasi-government entity, this could be formalised within government for delegation and orchestration of cyber security authority that would encompass the development of robust CTI capabilities to include technology, structural governance and processes and skills enhancement (L. Wells, 2019, pers. comm., 15 June; N. Jones, 2019, pers. comm., 12 June; N. Toshio, 2018,

pers. comm., 3 September).

The chief cyber security strategist at a leading Japanese corporation observed that Japan has a unique challenge in that its employment system and intelligence community workforce development differ completely from those in the US and the UK. Japan still largely depends on a lifetime employment system in which an employee will start with a company and remain there until they retire. As a result, cyber security experts that have cut their teeth in the Japanese government or intelligence communities rarely move to the private sector or vice versa. JPCERT, as an established organisation for incident response, and NISC, established as the coordinating authority for cyber policy, have fewer resources than ministries in their budget for workforce development that affects the continuity of operations and knowledge management in cyber security (K. Fujisue, 2020, pers. comm., 7 March; N. Toshio, 2018, pers. comm., 3 September). Japan's challenges in resolving continuity and knowledge management issues are readily compared with the UK experience of setting up the National Cyber Security Centre (NCSC) in reconciling government and private sector organisational cultures (Hannigan, 2019). While more mature, the US cyber authority responsibility and accountability structure has sought through its maturation to define the lines between interested government entities and raise cyber acumen, particularly in threat hunting which is a preoccupying theme of the US Cyberspace Solarium Commission in its recommendations for strengthening US cyber defence (King and Gallagher, 2020). US and UK cyber and intelligence professionals and government officials have noted the need to have allies and partners like Japan that have comparable workforce cyber skills sets to maximise joint efforts, particularly in threat hunting and intelligence analysis. Therefore, there are efforts across military entities in the US, UK and Japan to equalise cyber acumen. While noting that no two organisations (or nations) handle cyber threats in the same way, workforce structures have a role in robust national threat intelligence capabilities. NATO may have a role here as a 'boundary entity' (Wagner et al, 2019) in defining a 'common operating language' and activating the global cyber defence knowledge ecosystem toward more effective CTI sharing.

C. Challenge Three: Understanding each other

Dunn Cavelty and Egloff (2019, pg. 41) explain 'cybersecurity governance' as 'a risk management approach based on continuous monitoring, measurement and control [...seeking to] establish trust and stability of expectations among different actors' as originally defined by Bowen et al. (2006). The key phrase here is 'stability of expectations'. For threat intelligence shay ring, this means knowing that information exchanged will be safeguarded and acted upon in a timeframe useful for attribution. It is unrealistic–and perhaps unnecessary (Stevens, 2017)–to expect countries to adopt parallel structures, legislation and authorities. It is practically useful to the urgent task at hand for partners to agree on metrics and standards by which cyber security risk is minimised: in other words, 'we don't really mind how you do it, we just want to know that it has been done in a way that our systems and organisation can understand and engage with, at the moment when we need

to work together'. Creating this common operating language based around a requirement to act on threat information may facilitate the rapid exchange of expertise and threat intelligence.

The obligations, permissions and preferences of countries collectively shape their global relations (Stevens, 2012), organisational cultures and national strategic culture. Strategic culture is strongly influenced by context: no state (or company) forms a cyber defence posture in isolation; experience of past success and failures contributes to shaping policy and actions. NATO's approach to cyber is rooted in the experience of adaptation to the security environment of the 1990s, cyber attacks on NATO operations in 1999 and security alliances of the post-9/11 era (Burton, 2015; Healey and Jordan, 2014). This same mindset applies today in building an approach to yet another challenge in the international security environment. In building and projecting a cyber defence posture, countries are influenced by world events, institutional memory and geopolitical imagination. US doctrine on information warfare emerged in the wake of Operation Desert Storm (Stevens, 2012) and the cyber attacks of 2006, while the cyber security political imagination of the US has been shaped by events such as Stuxnet (Stevens, 2018), the Office of Personnel Management (OPM) breach and the indictment of APT10. For Japan, 'year zero' was the 2011 attacks on Mitsubishi Heavy Industries (Kallender 2014), echoed in another attack on Mitsubishi in May 2020 (CSIS, 2020). In 2011, Japan's Ministry of Economy, Trade and Industry (METI) reported nearly 37 per cent of Advanced Persistent Threats (APTs) were focused on Japan's infrastructure, notably industrial control systems in power plants and manufacturing facilities (Kallender 2014). The UK is preoccupied with countering financial crimes and containing the cyber threat from Russia. These experiences collectively shape how Japan, the UK and the US approach the task of threat intelligence collection and sharing.

The US hopes that encouraging acceptable international behaviours in cyberspace will be more consistent with a shift in paradigm from mere deterrence to persistent engagement for seizing and gaining the operational advantage by actively engaging and contesting cyber behaviour by adversaries (Lopez, 2019; Miller and Pollard, 2019; Harknett, 2018). In seeking to 'remake cyberspace in its own image' (Segal, 2018: p. 10) through overseas investment in infrastructure and influence in international standards, China also effectively delivers a deterrent effect (Economist Intelligence Unit, 2017). Japan's entire approach to cyber security is limited by its pacifist constitution (Matsubara, 2018a) which contributes to hesitation in cyber attack attribution that is thought to potentially provoke retaliation or escalation to war (Nakasone, 2020). The UK's tendency to debate but then largely disregard parliamentary committee review outcomes across successive parliaments has the potential to render new legislation of little effect against embedded and persistent adversaries (Clarke and Knake, 2020; Intelligence and Security Committee of Parliament, 2020). Nations do not always act alike in response to the same threat (Ferguson, 2011; Stone, 2005), so understanding a partner's strategic culture can significantly improve the chances of success in joint working arrangements: indeed, one outcome

of our interviews and research to date has been a modest contribution to understanding how our partners and allies think. Ablon et al. (2019) in their study for RAND have suggested that establishing a standardised Indications and Warning (I&W) model across NATO allies and partners should be a priority for nations to ensure their effective military presence in cyberspace. Building a 'common operating language' for threat intelligence sharing should include identifying where strategic cultures converge (and where they do not) because this helps in defining a minimum viable architecture for collaboration. This complexity in the translation of classification from sender to receiver further adds to the lag time in synthesising critical information to counter cyber threats and actual attacks—the cyber equivalent of having to pull out a dictionary in the middle of a live conflict. These deficiencies and incompatibilities prolong and complicate attribution and assessment of if and how domestic infrastructures were used or weaponised by an adversary.

The recent development in the US approach to CNI protection is key in re-evaluating how we conceptualise accountability, cyber risk and resilience because it considers capabilities across sectors and national critical functions, rather than stove-piping within industries. This approach finds ready comparison with the founding principles of NATO: while the Treaty does not name any specific threat or adversary, it does establish the 'operating principles for a defensive alliance' (Olsen, 2020, p. 5), which have not needed modification despite the growth of the Alliance to include a much more diverse membership than at its inception. The UK is also moving toward consideration of critical systems (akin to functions) and assessing their vulnerability to cascading risks,[6] a practice generally less formalised in government but vital for characterising the environment in which threat intelligence must perform (Wells et al., 2017). Identifying a 'common operating language' for threat intelligence sharing, including identifying and aligning where strategic culture and governance tools converge (and where they do not) can help to define a minimum viable architecture for international collaboration.

4. CONSIDERATIONS FOR NATO

Reviewing collaboration agreements between the UK, Japan and the US since 2008 we find an emphasis on action outstanding. In particular, the experiences of Japan illustrate that domestic infrastructure must be in place to effectively enable CTI sharing among internal government and private sector entities that can be leveraged for external communication to allied and partner nations. Even though the technologies exist in Japan to support more robust CTI, strategic culture plays a role in constraining how, where and by whom intelligence can be shared and acted upon. For example, some constraints stem from privacy and trust issues between the public and private sector, how expertise in work is traditionally developed impacting cyber skillset development, and fears associated with potential retaliation from active attribution or offensive cyber operations. Domestic laws can also constrain

[6] See e.g. CRUISSE Project, a research consortium with the National Security Secretariat of the UK Cabinet Office (NSS, UK Cabinet Office, 2019).

capability developments particularly those that do not provide needed cyber security legal authority to those government entities that establish policy, which also undercuts funding for cyber authorities and limits capability for workforce development. Insights from Japan's experiences in adapting to global cyber threats suggests an imperative to understand these differences across nations and seek methods to overcome these barriers.

While the requirement for multinational cyber cooperation is challenged by unbalanced technical capabilities, strategic cultures and legal frameworks, NATO is well-positioned to enable partner and allied nations to share CTI, particularly by assisting with enabling use of its MISP and encouraging best practice in provisioning cyber authority structures for threat intelligence sharing as part of a potential international cyber security maturity, resilience development and assessment programme. For this programme, the NATO Cooperative Cyber Defence Centre of Excellence could take the lead in:

> (1) reconciling incompatibilities and promoting level setting of threat intelligence capabilities across partner and allied nations to speed the flow of information;
>
> (2) coordinating agreements to ensure trusted threat intelligence information is acted upon;
>
> (3) enabling partners and allied countries to adopt a minimal set of classification standards, compatible ontologies and comparable personnel security clearances management programs that enable threat intelligence sharing;
>
> (4) encouraging the development of a threat intelligence maturity scale that addresses technology, process, and workforce capabilities to aid nations in readily identifying specific improvements to benefit the international threat intelligence ecosystem; and
>
> (5) developing mechanisms to promote accountability in global industries to build threat intelligence capacity and trusted sharing with public entities for the international cyber mission.

Making CTI sharing viable requires that partner nations start talking the same language and allow for some compromise on blaming, naming and shaming, to encourage the private sector to take more responsibility and contribute to the national cyber mission of their respective governments. Implications for NATO partnerships include identifying structures and practices among partners that are not constrained by strategic culture and exploring the scope for NATO's role—as a non-state actor—in defining a 'common operating language' for CTI architectures and practices. Building comparable threat intelligence capabilities under the constraints we have identified in this study is extremely difficult. Yet, the requirement to accelerate and facilitate effective global cooperation in cyber defence is urgent. Thus, in undertaking this charge NATO can truly be unfettered in deliberation to thwart the ability of any entity to weaponise the cyberspace domain.

5. ACKNOWLEDGEMENTS

This chapter presents selected insights from research conducted over two years, supported in part by the Abe Fellows Programme and the US Social Sciences Research Council. The authors gratefully acknowledge the perspectives given by cyber security practitioners and officials in the US, Japan and the UK. The views are the authors' own interpretations and do not represent the official positions of Japan, the US, UK or organisations with whom we are affiliated or engaged with during this study.

6. REFERENCES

Abe, D. (2020) 'Lagging China and the US, Japan to Beef up Cyber Defense'. *NikkeiAsia.* Available at: https://asia.nikkei.com/Politics/Lagging-China-and-the-US-Japan-to-beef-up-cyberdefense [Accessed: 30th September 2020].

Abe, D. and Rieko, M. (2020) 'Defense Minister Taro Kono speaks during an interview on Aug. 12 in Tokyo'. *NikkeiAsia*. Available at: https://asia.nikkei.com/Editor-s-Picks/Interview/Japan-wants-de-facto-Six-Eyes-intelligence-status-defense-chief

Ablon, L. et al. (2019) *Operationalising Cyberspace as a Military Domain: Lessons for NATO*. RAND Corporation. Available at: https://www.rand.org/pubs/perspectives/PE329.html [Accessed: 13th August 2020].

Afina, Y., Inverarity, C. and Unal, B. (2020) *Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems*. London: Royal Institute of International Affairs. Available at: https://www.chathamhouse.org/publication/cyber-resilience-nato-command-control-communication-afina-inverarity-unal.

Baezner, M. and Cordey, S. (2019) *National Cyber security Strategies in Comparison – Challenges for Switzerland*. Zurich: Center for Security Studies (CSS), ETH Zürich.

Bowen, P., Hash, J. and Wilson, M. (2006) *Special Publication 800-100. Information Security Handbook: A Guide for Managers* (Gaithersburg: National Institute of Standards and Technology (NIST), 2006), p.6.

Burton, J. (2015) 'NATO's cyber defence: strategic challenges and institutional adaptation'. *Defence Studies*. 15(4), pp. 297–319.

Center for Strategic Information Studies (2020) 'CSIS Significant Cyber Incidents'. *CSIS website*. Available at: https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents [Accessed: 24 July 2020].

Chesney, R. (2016) 'A Primer on Apple's Brief in the San Bernadino iPhone Fight'. *Lawfare.* Available at: https://www.lawfareblog.com/primer-apples-brief-san-bernadino-iphone-fight [Accessed: 26th September 2020].

Clarke, R. A. and Knake, R. K. (2020) *The Fifth Domain*. New York: Penguin Random House.

Dunn Cavelty, M. and Egloff, F. J. (2019) 'The Politics of Cybersecurity: Balancing Different Roles of the State'. *St Antony's International Review*. 15(1), pp. 37–57.

Economist Intelligence Unit (2017) *China Going Global*. London. Available at: https://www.eiu.com/public/topical_report.aspx?campaignid=ChinaGoingGlobal [Accessed: 13th August 2020].

Economist Intelligence Unit (2018) *World risk: Alert – Global risk scenarios*, *Risk Briefing*. London. Available at: http://viewswire.eiu.com/index.asp?layout=RKArticleVW3&article_id=1876319171 [Accessed: 8th August 2020].

Economist Intelligence Unit (2019) *Cause for concern? The top 10 risks to the global economy 2019*. London. Available at: https://pages.eiu.com/rs/753-RIQ-438/images/Global_risks_2019.pdf [Accessed: 8th August 2020].

European Parliament (2018) 'Report on Cyber Defence'. Available at: https://www.europarl.europa.eu/doceo/document/A-8-2018-0189_EN.html [Accessed: 8th August 2020].

Feldman, L. and G. Witte (2017) 'Cyber threat intelligence and information sharing'. National Institute of Standards Information Technology Labs Bulletin. Available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=923332 [Accessed: 25th September 2020].

Ferguson, J. (2011) 'The U.S.-Japan Alliance and Russia', in Inoguchi, T., Ikenberry, G. J., and Sato, Y. (eds) *The U.S.-Japan Security Alliance*. New York: Palgrave Macmillan US, pp. 195–216.

Gady, F. and Y. Koshino (2020) 'Japan and cyber capabilities: how much is enough?'. Available at: https://www.iiss.org/blogs/military-balance/2020/08/japan-cyber-capabilities [Accessed: 25th September 2020].

Government of Japan (2017) 'The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)'. Available at: http://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf [Accessed: 13th August 2020].

Hannigan, R. (2019) 'Organising a Government for Cyber'. *Royal United Services Institute for Defence and Security Studies*. Available at: https://rusi.org/sites/default/files/20190227_hannigan_final_web.pdf [Accessed: 24th July 2020].

Hansen, L. and Nissenbaum, H. (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School'. *International Studies Quarterly*. 53(4), pp. 1155–1175.

Harknett, R. (2018) 'United States Cyber Command's New Vision: What It Entails and Why It Matters,' Lawfare. Available at: https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters [Accessed: 26th September 2020].

Harknett, R. and Smeets, M. (2020) 'Cyber campaigns and strategic outcomes'. *Journal of Strategic Studies*. March 2020, pp.1-34.

Healey, J. and Jordan, K.T. (2014) 'NATO's Cyber Capabilities: Yesterday, today, and tomorrow'. Issue Brief, September 2014, Atlantic Council.

Intelligence and Security Committee of Parliament (2020) *Russia*. HC632. London: UK Government.

Kallender, P. (2014) 'Japan, the Ministry of Defense and Cyber-Security: Progress and Pitfalls'. *The RUSI Journal*. 159(1), pp. 94–103.

King, A. and Gallagher, M. (2020) 'US Cyberspace Solarium Commission Report'. *US Cyber Solarium Commission website*. Available at: https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view [Accessed: 24th July 2020].

Kolini, F. and Janczewski, L. (2017) 'Clustering and Topic Modelling: A New Approach for Analysis of National Cybersecurity Strategies'. *PACIS 2017 Proceedings*. Available at: https://aisel.aisnet.org/pacis2017/126 [Accessed: 24th July 2020].

Kono, K. (2015), 'A Japanese Perspective on Deterrence in Cyberspace Grey Zone Contingencies and the Role of the Japan-U.S. Alliance' in W. Harold, S. *et al.* (2015) 'The U.S.-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains'. Rand Corporation: Santa Monica.

Koepke, P. (2017), 'Cybersecurity information sharing incentives and barriers'. CISL Working Paper 2017-13. MIT Sloan School of Management.

Kuerbis, B. and Badiei, F. (2017) 'Mapping the cybersecurity institutional landscape'. *Digital Policy, Regulation and Governance*. 19(6), pp. 466–492.

Kyodo, J. (2019) 'U.S. to defend Japan from cyberattack under security pact'. *Japan Times*. Available at: https://www.japantimes.co.jp/news/2019/04/20/national/politics-diplomacy/first-japan-u-s-say-security-treaty-cover-cyberattacks/ [Accessed: 24th July 2020].

Lewis, J. (2015) 'U.S.-Japan Cooperation in Cybersecurity'. CSIS publication. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151105_Lewis_USJapanCyber_Web.pdf [Accessed: 23rd July 2020].

Lopez, T. (2019) 'Persistent Engagement, Partnerships, Top CYBERCOM's Priorities,' US DOD https://www.defense.gov/Explore/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/ [Accessed: 24th July 2020].

Luiijf, E., Besseling, K. and Graaf, P. D. (2013) 'Nineteen national cyber security strategies'. *International Journal of Critical Infrastructures*. 9(1/2), p. 3.

Malware Information Sharing Program (MISP) (2020) 'MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing'. *MISP Threat Sharing website*. Available at: https://www.misp-project.org/index.html [Accessed: 24 July 2020].

Matsubara, M. (2018a) 'How Japan's New Cybersecurity Strategy Will Bring the Country Up to Par with the Rest of the World'. *Council on Foreign Relations*. Available at: https://www.cfr.org/blog/how-japans-new-cyber security-strategy-will-bring-country-par-rest-world [Accessed: 13th August 2020].

Matsubara, M. (2018b) 'How Japan's Pacifist Constitution Shapes Its Approach to Cyberspace'. *Council on Foreign Relations*. Available at: https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace [Accessed: 13 August 2020].

Miller, J. and N. Pollard (2019) 'Persistent Engagement, Agreed Competition and Deterrence in Cyberspace'. *Lawfare*. Available at: https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace [Accessed: 26th September 2020].

Ministry of Defense (MOD) (2018) 'Security Surrounding Japan: Section 5 Trends in Cyberspace'. Available at: https://www.mod.go.jp/e/publ/w_paper/pdf/2018/DOJ2018_1-3-5_web.pdf [Accessed: 30 September 2020].

Nakasone, Y. (2020) *Japan – A State Strategy for the Twenty-First Century*. 1st edn. London: Routledge. Doi: 10.4324/9781315029467.

National Security Secretariat (NSS) UK Cabinet Office (2019) 'CRUISSE Pilot–Identifying and Addressing Uncertainties in the UK's Cyber Risk Landscape'. *NSS website.* Available at: http://cruisse.ac.uk/wp-content/uploads/2019/02/CO-Project-Final-Report-v2.pdf [Accessed: 24 July 2020].

NATO (2019) 'Remarks by NATO Secretary General Jens Stoltenberg at the

Cyber Defence Pledge Conference, London'. *North Atlantic Treaty Organisation website*. Available at: https://www.nato.int/cps/en/natohq/opinions_166039.htm [Accessed: 8th August 2020].

NATO (2020) 'Secretary General commends strong cooperation between NATO and Japan'. *North Atlantic Treaty Organisation website*. Available at: http://www.nato.int/cps/en/natohq/news_177380.htm [Accessed: 11th August 2020].

NATO Communications and Information Agency (NCIA) (2018) 'New NATO-Industry cyber partnerships signed at NITEC18'. *NATO CIA website*. Available at: https://www.ncia.nato.int/about-us/newsroom/new-natoindustry-cyber-partnerships-signed-at-nitec18.html [Accessed: 24th July 2020].

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2017) 'NotPetya and WannaCry Call for a Joint Response from International Community'. *NATO CCCDOE website*. Available at: https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/ [Accessed: 8th August 2020].

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2020) 'National Cyber Security Strategies by Country, *Strategy and Governance Documents Library.' NATO CCDCOE website*. Available at: https://ccdcoe.org/library/strategy-and-governance/ [Accessed: 24th July 2020].

Nippon Electric Company (NEC) (2017) '5 Reasons Why Japan Fell Behind in Cybersecurity'. *NEC Wisdom for Business Leaders.* Available at: https://wisdom.nec.com/en/technology/2017120601/index.html [Accessed: 26th September 2020].

Menges, F., Sperl C., and Pernul G. (2019) 'Unifying Cyber Threat Intelligence'. In: Gritzalis S., Weippl E., Katsikas S., Anderst-Kotsis G., Tjoa A., Khalil I. (eds) Trust, Privacy and Security in Digital Business. Lecture Notes in Computer Science, vol 11711. Springer.

Ministry of Foreign Affairs of Japan (MOFA) (2005) 'Agreement between the Governments of Japan and the United States of America Concerning Security Measures for the Protection of Classified Military Information'. Available at: https://www.mofa.go.jp/region/n-america/us/security/agree0708.html [Accessed: 30th September 2020].

Naughton, J. (2016) 'The evolution of the Internet: from military experiment to General Purpose Technology'. *Journal of Cyber Policy*, 1(1). pp. 5–28.

Olsen, J. (2020) 'Understanding NATO'. *The RUSI Journal*, 165(3). pp. 60–72.

Pernik, P. (2014) 'Improving Cyber Security: NATO and the EU'. International Centre for Defence Studies.

Schinagl, S. and Shahim, A. (2020) 'What do we know about information security governance? 'From the basement to the boardroom': towards digital security governance'. *Information and Computer Security*. 28(2), pp. 261–292.

Segal, A. (2018) 'When China Rules the Web'. *Foreign Affairs*, September/October. Available at: https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web [Accessed: 13th August 2020].

Shackelford, S. J. and Kastelic, A. (2015) 'Toward a State-Centric Cyber Peace?: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity'. *New York University Journal of Legislation and Public Policy*. 18(4), pp. 895–984. Available at: https://medium.com/freeman-spogli-institute-for-international-studies/bytes-bombs-and-spies-261564d51157 [Accessed: 25th September 2020].

Smeets, M. and H. Lin (2019). 'Chapter 4: A Strategic Assessment of the U.S. Cyber Command Vision,' in Lin, H., & Zegart, A. (Eds.). (2019). Bytes, Bombs, and Spies: The strategic dimensions of offensive cyber operations. Brookings Institution Press. Available at: https://medium.com/freeman-spogli-institute-for-international-studies/bytes-bombs-and-spies-261564d51157 [Accessed: 25th September 2020].

Stevens, T. (2012) 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace'. *Contemporary Security Policy*. 33(1), pp. 148–170.

Stevens, T. (2017) 'Cyberweapons: an emerging global governance architecture'. *Palgrave Communications*. 3(1), p. 16102.

Stevens, T. (2018) 'Cyberweapons: power and the governance of the invisible'. *International Politics*. 55(3–4), pp. 482–502.

Štitilis, D., Pakutinskas, P. and Malinauskaitė, I. (2017) 'EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis'. *Security Journal*. 30(4), pp. 1151–1168.

Stone, E. et al. (2005) *Report of Comparative Strategic Cultures Workshop (phase 1)*. Fort Belvoir: US Defense Threat Reduction Agency. Available at: https://www.files.ethz.ch/isn/129010/comparativestrategicculturesworkshop.pdf [Accessed: 8th August 2020].

Tabuchi, H. (2011) 'U.S. Expresses Concern About New Cyberattacks in Japan'. *The New York Times*. Available at: https://www.nytimes.com/2011/09/22/world/asia/us-expresses-concern-over-cyberattacks-in-japan.html [Accessed: 29th September 2020].

Tolga, İ. (2019) 'Whole-of-Government Cyber Information Sharing'. *NATO Cooperative Cyber Defence Centre of Excellence*. Available at: https://ccdcoe.org/uploads/2019/06/Cyber_Info_Sharing_Ihsan_Tolga_CCDCOE_June_2019-.pdf [Accessed: 24th July 2020].

Tsuchiya, M. (2019) 'A difficult road to international norms for cybersecurity'. *Nihon Keizai Shinbun*, 27 November. Available at: https://www.nikkei.com/article/DGXMZO52628790W9A121C1945M00/ [Accessed: 13th August 2020].

US Department of Defense, 'The Guidelines for U.S.-Japan Defense Cooperation'. April 27, 2015. https://archive.defense.gov/pubs/20150427_--_GUIDELINES_FOR_US-JAPAN_DEFENSE_COOPERATION.pdf [Accessed: 24th July 2020].

114th US Congress (2015) *Cybersecurity Information Sharing Act of 2015 ('CISA')*. Available at: https://www.congress.gov/bill/114th-congress/senate-bill/754 [Accessed: 30 Sept 2020].

von Solms, B. and von Solms, R. (2018) 'Cybersecurity and information security – what goes where?'. *Information and Computer Security*. 26(1), pp. 2–9.

von Solms, R. and van Niekerk, J. (2013) 'From information security to cyber security'. *Computers & Security*. 38, pp. 97–102.

Wagner, T., Mahbub, K., Palomar, E. and Abdallah, A. (2019) 'Cyber threat intelligence sharing: Survey and research directions'. *Computers & Security*. 87, pp.1-13.

Weiss, M. and Jankauskas, V. (2019) 'Securing cyberspace: How states design governance arrangements'. *Governance*. 32(2), pp. 259–275.

Weaver, N. (2020) 'Apple vs FBI: Pensacola Isn't San Bernardino'. *Lawfare*. Available at: https://www.lawfareblog.com/apple-vs-fbi-pensacola-isnt-san-bernardino [Accessed: 25th September 2020]

Wells II, L., Tsuchiya, M. and Repko, R. (2017) *Improving Cybersecurity Cooperation between the Governments of the United States and Japan*. Washington, DC: Sasekawa Peace Foundation USA. Available at: https://spfusa.org/wp-content/uploads/2017/02/Improved-Cyber security-cooperation.pdf [Accessed: 24th July 2020].

7. APPENDIX I. INTERVIEWEES AND RESEARCH METHODS SUMMARY

Japan Cyber Authorities or Related Entities		
Prime Minister Advisor	Senior level primary advisor on IT policy	1
Japan's Minister of House of Councillors	Senior representatives from the Minister of Cyber Security	3
Japan's National Centre of Incident Readiness and Cyber security (NISC)	Senior policy and mid-level analysts	5
Japan Computer Emergency Response Team (JPCERT)	Current and former mid-level personnel	3
National Institute of Communication and Technology (NICT)	Member of the National Cyber security Research Institute	1
Japan Ministry of Defence (MOD)	Senior level cyber operations and policy military officers (05-06)	3
Ministry of Economy, Trade, and Industry (METI)	Senior level current and former members for cyber security related standards	3
Ministry of Education, Culture, Sports, Science and Technology (MEXT)	Senior level personnel on IT policy	1
Ministry of Internal Affairs and Communication (MIC)	Senior level former members for ICT policy	1
Information-Technology Promotion Agency, Japan (IPA)	Mid-level personnel	2
National Policy Agency (NPA) Office of Intelligence for Cyber, Security Planning Division	Senior and mid-level technicians	3
IT-Information Sharing and Analysis Centres for Information Technology and Information Communication Technology	Senior policy and member personnel	4
Cyber Policy Academic Research	Professors in Cyber policy and ministry advisors on cyber research at Keio University	5

UK Cyber Authorities or Related Entities		
National Cyber Security Centre (NCSC)	Technical Director NCSC Professors in the Academic Centre of Excellence in Cyber Security Research (ACE-CSR) sponsored by NCSC programme at Royal University and Imperial College London partnered with US and Japan (Keio) Universities for an International Cyber Strategy Curriculum	1 2
European Union Agency for Cyber security	Senior policy and member personnel	2
INTERPOL	Member of the cyber crime Threat Response team, Cyber Fusion Centre	1
UK Ministry of Defence	Senior officers in the Joint Forces Cyber Group Policy and Plans	2
EUROPOL	Former Executive Director	1
US Cyber Authorities or Related Entities		
US Department of Defense	Advisor to DoD CIO US Air Force CISO US Air Force Chief DevSecOps US Navy SES and military officers (05-Flag) in Cyber Policy and Planning US CYBERCOM senior personnel in policy and plans	1 1 1 5 2
Cybersecurity and Infrastructure Security Agency (CISA)	International liaisons	2
HQ FBI Cyber Division and Regional Office	Senior Intel Officer and Supervisory agents	5
Former US Presidential Administration Personnel involved in Cyber Strategy Development	Former Director of National Intelligence Former Principal Deputy Assistant Secretary of Defense	1 1
Other Cyber Relevant Entities		
Private sector organisations involved Japan, US, and UK cyber operations (e.g., Toyota, Fujitsu, NEC, Hitachi, Squire Patton Boggs, Microsoft, Northrop Grumman, KPMG, PwC)	General Manager, Senior analysts, security solutions managers, legal counsel on cyber	10
Cyber security Consulting Firms (CrowdStrike, Fire Eye, McAfee, Kaspersky)	Senior threat intelligence advisors	7
Total		80

Imagining and Anticipating Cyber Futures with Games

Andreas Haggman[1]
Head of Cyber Advocacy
UK government department

Abstract: This short chapter considers the relationship between games and futures, with specific focus on cyber security. Games and gamification have received renewed attention in both academia and industry over the past ten years. Within this broad field, the genre of wargaming occupies a significant but often underappreciated space.

Unlike what some observers might argue, wargaming is not just an activity for history anoraks with an overly keen interest in the past. Wargaming can indeed be used to better understand historical events, but it can also be used to explore the dynamics of the present or employed as a highly imperfect crystal ball to gaze into the future. When done right, wargaming can be a powerful tool to engage audiences with little subject matter expertise or game playing experience.

Three core arguments are made in this chapter. First, wargames can provide structure for players to imagine futures. Second, wargames can prepare players for the future by enabling them to anticipate emotions. Lastly, cyber wargames should avoid the trap of becoming enamoured with the technology of cyber security.

The chapter is grounded in diverse literature, drawing on material from cultural studies, strategic studies, modelling and simulation and history. Readers will find theoretical insights into the uses of games alongside practical advice for those seeking to use wargames in a cyber security context.

Keywords: *Cyber, multi-domain, cross-domain, concepts, Russia, China*

[1] Disclaimer: This work represents the personal opinions of the author. This work does not represent the opinion of the UK government and nothing in this document should be construed as UK government policy nor UK government endorsement of the work.

1. INTRODUCTION

Beyond frivolous entertainment, games have practical uses that are often overlooked. Wargaming is a genre of games and gamification that focuses on scenarios involving conflict. Conflict is not limited to direct military confrontation—a primary area of interest for NATO—but can encompass any situation where competition or strife is prevalent.

In cyberspace, current conflict is best characterised as ongoing competition below the level of military confrontation. State actors are continually jostling for position on adversaries' networks, seeking to maintain a foothold without causing undue disruption. Meanwhile, non-state hostile actors, such as organised crime groups, are running campaigns targeting private companies for financial gain.

For many people, cyber wargames conjure a vision of large-scale capture-the-flag events where teams of technical experts attempt to attack and defend their computer networks. Such exercises mimic the conflict we see in cyberspace, but in focusing on technology and tactics, the political and strategic dimensions of cyber security and cyber conflict are often missed. Participants learn how to defend against an attack, but they are not challenged to ask why an attack might occur in the first place.

In the cyber domain, NATO has been an active proponent of exercises, including Locked Shields and Crossed Swords. While both events focus on the technical side of cyber security—the former on strategic decision-making and the latter on operational aspects—these exercises have developed over time to include non-technical elements like legal and public relations. This suggests that the culture in NATO is amenable to using types of games outside the classic conception of a cyber wargame.

Wargames that remove the technical barrier allow participants from a broader range of backgrounds to contribute insight. Even deceptively simple wargames can be effective at prompting participants to imagine and convey futures in a focused way. By sharing these conceptions with other participants, wargaming sessions can result in a joined-up appreciation of future threats. Wargaming, most simply defined, is a 'model or simulation [...] whose sequence of events affects and is, in turn, affected by players representing the opposing sides' (Curry, 2011: p. 157). In this seminar definition, Peter Perla originally referred explicitly to warfare, but the concept can be extended to almost any instance of conflict, both inside and outside military domains. Whatever the activity portrayed, whether it is manoeuvring armoured vehicles or making a business investment decision, wargaming is ultimately focused on the human participants and their actions and experiences.

Throughout this chapter, the author seeks to promote the idea that in cyber security, a simple wargame can go a long way. Tabletop exercises are perhaps the ultimate in simplicity, but often fail to go beyond superficial what-if

scenarios and can deteriorate into unproductive 'Bunch of Gals/Guys Sitting Around a Table' (BOGSATs). Wargaming as a method is replete with tools and techniques that are effective at creating realistic scenarios and generate a high level of player engagement. Matrix games, for example, are types of wargames that bring structure and competition to tabletop exercises through the use of expert adjudication (akin to a professional 'Dungeon Master') and a modicum of gaming paraphernalia such as dice or cards. The author's own experience with a cyber strategy wargame is outlined in Section Five.

This chapter explores one particular dimension of wargaming: how it engages the forward-looking faculties of participants, specifically focusing on imagination and anticipation. In Section Two, the links between games and imagination are explored, with close reference to effective methods for enabling players to imagine futures at a political or strategic level. Section Three extends this discussion to anticipation and how games can emotionally prepare players for the future. Section Four considers the uncertain future of cyber capabilities, before section Five concludes with some actionable takeaways for the reader.

2. FUTURES AND IMAGINATION

The further we seek to gaze into the future, the more we have to employ our imaginative rather than our analytical faculties because of the increased uncertainty. Just consider science fiction literature, which often seems to become more far-fetched the further into the future it is set. At the same time, futures imagined on a shorter time frame can often be realistic; consider the apparent prescience of some of the works from authors like H. G. Wells (1908).

When we play games, we exercise our ability to imagine the future because we need to imagine the context in which future game actions will take place. After studying competitive chess players, Gary Fine (2014) concluded that players' strategy, consisting of a series of planned moves—or 'the line'—is the core mechanic in that game, not the moves themselves (p. 323). These 'lines' require an ability to anticipate the opponent's strategy to construct the imagined game future.

Chess, however, is a highly abstract game and teaches us little about contemporary strategy or politics. In his later life, political theorist Guy Debord attempted to amalgamate the imaginative capacities of wargaming with his leftist political ideals. His Game of War set out to capture the struggle between a bleak 'historical present' and an unattainable future of 'utopian imagination' (Galloway, 2009: pp. 151-152). Ultimately, Debord became obsessed with 'the sublimation of antagonistic desire into an abstract rulebook' and Game of War ended up as something which looked more like chess with some added mechanics around military logistics than a game of political strife (Galloway, 2009: p. 28).

Perhaps Debord, and others seeking to invoke imagined futures, can learn from Pericles of ancient Athens. Pericles was a master orator, able to convincingly convey potential futures to spur Athenians to action. What made Periclean futures so potent was their grounding in reality. According to Lawrence Freedman (2013), Pericles drew 'from an existing reality but moved beyond it' and the plausibility of a future was 'derived from its practicability' (p. 49). As an example, in cyber security, a future where only friendly actors derive the benefits from a technology like quantum computing seems more Debordian than Periclean. Instead, an imagined future involving quantum computing must consider the viability of this technology also being in the hands of hostile actors.

When designing wargames, the key to success is to understand the purpose of the game and the future it is intended to explore. A tactical awareness training tool might lend itself to a chess-like design where players can imagine 'lines' such as hopping from node to node while penetrating a network. Conversely, a strategic game exploring international political dimensions may need less of a strict rule set and instead provide realistic foundations for players to extrapolate their own imagined futures.

3. Futures and Anticipation

As an extension of imagining futures, anticipation has been described by Vincanne Adams et al. (2009) as 'an epistemic orientation towards the future' (p. 254). In other words, anticipating futures involves creating knowledge about the future, thereby negating surprise. In everyday usage, 'surprise' can be used either positively or negatively—compare a surprise birthday party to a surprise conference paper rejection. Wargaming is often concerned with negating negative surprises. David Hulse et al. (2016) identify that a core use of modelling (closely allied to wargaming) is understanding 'when, where and how "reducible ignorance" can be most effectually reduced vis-a-vis anticipated surprises' (p. 41). As tools for anticipating futures, wargames enable knowledge creation which can help reduce surprise.

An important aspect of anticipation is the emotion contained within surprises. A birthday party is a pleasant surprise, while a paper rejection is unpleasant. When it comes to drivers of human behaviour, Roy Baumeister et al. (2007) attest that 'anticipation of emotion is more important than the actual emotion' (p. 174). While writing a paper, an author might contemplate the hurt associated with rejection and be compelled to make a greater effort to write a brilliant paper.

Because of its ludic nature, wargaming is closely associated with competition and personal performance. Wargames usually have winners and losers; the winners experience joy, elation and satisfaction, the losers are disappointed, angry and dissatisfied. One of the insidious features of wargaming is that players' in-game behaviour can be driven by anticipation of these emotions, rather than reasoned actions. However, the other side of this coin is that

players become better prepared for the future by anticipating and eventually experiencing these emotions in the safety of the game environment. Wargames can help desensitise players to the extremes of emotions contained within surprises—or, indeed, other adverse experiences such as frustration, confusion, information deficiency or excess—so that when they encounter similar surprises and emotions in real life, the effects on their behaviour are not as drastic.

4. CYBER FUTURES

As domains of warfare have increased from two (land and sea), to three (air), to four (cyberspace) and five (space) (NATO, 2020), wargaming has been increasingly challenged to tackle the technological developments of the day. Sharon Ghamari-Tabrizi (2000) writes that during the Cold War, 'the technical horizon within which future wars would be fought would change constantly, albeit uncertainly' (p. 164). In the Cold War context, nuclear weapons dominated wargaming scenarios, yet the 'technical horizon' did not fluctuate as wildly as game designers of the time might have envisaged. With the benefit of hindsight, we can say that nuclear weapons of greater yields could be delivered further and faster in the 1980s than the 1950s, but the overall nature of these weapons did not change, and indeed remains the same today.

With cyber capabilities, wargaming finds itself looking at another technical horizon. The past 15 years have only provided glimpses of what cyber operations might look like at full scale—Estonia in 2007, Stuxnet in 2010 and NotPetya in 2017 are excellent examples. It is possible to imagine a future where cities go dark as power plants are shut down at the whim of an adversary. Indeed, such doom-mongering has been successful at capturing public and political attention—not dissimilar from the scenarios of the Cold War.

However, perhaps these examples are more than glimpses—do these totemic operations represent the zenith of cyber capabilities? It is possible to imagine a future not unlike today where cyber capabilities are used sparingly because of their expense and their limited and unpredictable effects.

Or perhaps both of these imagined futures are incorrect and cyber capabilities have yet to reveal their final form. In the early 20th century, reams of strategic thinking were expounded on the novel concept of airpower and yet the technology that prompted this thinking was airships, not aeroplanes—recall that the Wright Flyer first took off in 1903, and that Giulio Douhet's seminal The Command of the Air was not published until 1921. Strategic thinking around cyber has similarly boomed in the early 21st century, but cyber capabilities of the future may make Stuxnet look like an inflatable blimp by comparison. The point here is that it is difficult to know when, or even if, technology will outpace strategic thinking.

5. CYBER WARGAMING

When imagining and anticipating cyber futures, the lesson for wargaming is similar as for Wells' science fiction, Wells himself being an avid wargamer. In The War in the Air, Wells' characterisation of airpower was not wholly incorrect, though it was exaggerated because the technology in the novel was swiftly superseded. In cyber wargames, the technical aspects of cyber capabilities should be deemphasised and potential effects should be based on current observable reality rather than unsubstantiated hype.

That is not to say that cyber wargames should ignore technology. After all, cyber is a technical domain, not a natural one. But cyber wargames at the strategic level should not get bogged down in the relative merits of, say, ElGamal versus RSA encryption algorithms. Instead, the effect 'data is encrypted' would reasonably be the level of detail required for strategy games. By focusing away from the micro-level details of technology, participants in wargames can explore the macro-level strategic and political reasons why a cyber attack might occur and how to respond to it, without being burdened with the tactical minutiae of cyber security. These minutiae have their place in attack-defence exercises and capture-the-flag events, but these types of games do not readily lend themselves to the imaginative and anticipatory dimensions of wargaming.

From his experience of the 2010 Schriever Wargame organised by the US Air Force, George Foresman, former Undersecretary at the US Department of Homeland Security, stated that 'the lessons identified [...] are not futuristic concepts' (2010: p. 8). This sentiment seems to intimate a sweet spot for wargames to hit: create a scenario that participants can imagine as a plausible future and from which they can anticipate and learn lessons; but avoid a scenario that is overly 'futuristic' and which participants relegate to the realms of science fiction.

For those seeking to use wargames and who want to hit that sweet spot while avoiding the trappings of technology, a good starting point would be to keep it simple. A game does not necessarily need intricate graphics and advanced gameplay mechanics to be effective. For example, sample games found in Dark Guest (Curry & Rice, 2013) or The Handbook of Cyber Wargames (Curry & Drage, 2020) require only basic gaming paraphernalia – in many cases just a die. The real value comes from the players rather than the games themselves.

In the author's own experience, a cyber strategy wargame with a moderate degree of gaming paraphernalia has been successful at eliciting learning moments for players (Haggman, 2019). The game in question was loosely based on the UK National Cyber Security Strategy (HM Government, 2016) and used a game board, cards, dice, player characters and a set of rules to convey some limited detail about cyber security topics and dynamics. This was less simple than a matrix game but provided very direct discussion opportunities be-

cause players could assess the game components. Asking players what they would add to the game was often revealing in terms of what they understood to be important in cyber security, at both strategic and operational levels. Moreover, because the game was relatively easy to learn and purposely designed to be fun, it was highly engaging for players. Overcomplication can discourage player engagement. Simplicity incites imagination and anticipation, thereby realising the benefits associated with wargaming futures.

6. REFERENCES

Adams, V., Murphy, M. & Clarke, A. E. (2009) Anticipation: Technoscience, life, affect, temporality. *Subjectivity*. 8, 246-265.

Baumeister, R. F., Vohs, K. D., DeWall, C. N. & Zhang, L. (2007) How Emotion Shapes Behavior: Feedback, Anticipation, and Reflection, Rather Than Direct Causation. *Personality and Social Psychology Review*. 11 (2), 167-203.

Curry, J. (2011) *Peter Perla's The Art of Wargaming: A Guide for Professionals and Hobbyists*. The History of Wargaming Project.

Curry, J. & Price, T. (2013) *Dark Guest: Training Games for Cyber Warfare Volume 1 –Wargaming Internet Based Attacks*, 2nd ed.

Curry, J. & Drage, N. (2020) T*he Handbook of Cyber Wargames: Wargaming the 21st Century.* The History of Wargaming Project.

Douhet, G. (1921) *The Command of the Air*. trans. Ferrari, D. Air University Press.

Fine, G. A. (2014) Strategy and Sociability - The Mind, the Body, and the Soul of Chess. *American Journal of Play.* 6 (3), 321-344.

Foresman, Hon. G. W. (2010) The Complexities of American National Security: Enabling A New Generation of Leadership. *High Frontier - The Journal for Space and Cyberspace Professionals.* 7 (1), 5-8.

Freedman, L. (2013) *Strategy: A History*. Oxford University Press.

Galloway, A. R. (2009) Debord's Nostalgic Algorithm. *Culture Machine*. 10, 131-156.

Ghamari-Tabrizi, S. (2000) Simulating the Unthinkable: Gaming Future War in the 1950s and 1960s. *Social Studies of Science*. 30 (2), 163- 223.

Haggman, A. (2019) 'Cyber Wargaming: Finding, Designing and Playing Wargames for Cyber Security Education'. PhD thesis, Royal Holloway University of London.

HM Government. (2016) 'National Cyber Security Strategy 2016-2021'. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. [Accessed 23rd October 2020].

Hulse, D., Branscomb, A., Enright, C., Johnson, B., Evers, C., Bolte, J. & Ager, A. (2016) Anticipating surprise: Using agent-based alternative futures simulation modeling to identify and map surprising fires in the Willamette Valley, Oregon USA. *Landscape and Urban Planning*. 156, 26-43.

NATO. (2020) 'NATO's approach to space'. Available at https://www.nato.int/cps/en/natohq/ topics_175419.htm. [Accessed 23rd October 2020].

Wells, H. G. (1908) *The War in the Air*. Available at: http://www.gutenberg.org/ebooks/780. [Accessed 23rd October 2020].

PART V:
Regulatory and Policy Responses to Cyber Security Challenges

Refocusing Export Control Regimes to Effectively Address Cyber Security Concerns

Cindy Whang
Assistant Professor
Department of Financial and Economic Law
Fu Jen Catholic University

Abstract: Cyber security as a common security interest of NATO member states raises the question of how to promote it through different technical and policy constructs. One such aspect has been through establishing trade regulations like export controls to prevent the proliferation of military-use goods and technology for national security reasons. Since NATO's formation, member states have used export controls as a trade measure to protect their national security. As cyber security threats have become an important feature of the protection of national security, the role by which export control regulations should be used to address this new rising threat should be discussed. Export control regimes have traditionally functioned as a means to prevent the proliferation of military-use and technological goods from crossing borders. The two primary elements used to achieve that goal were the use of export control lists to determine the subject of export control and the allocation of export control liability to the violating party. While the export control regulations regulated 'technology' as an entity, before the widespread use of the internet, the control and enforcement of this intangible form of technology were predicated on the technology being installed on physical goods. In addressing cyber security concerns through export control regimes, this paper analyses the construct of export control lists and the imposition of export liability through the lenses of cyber security concerns and argues that the current construct of export controls regulations might not be effective in addressing these concerns.

Keywords: *Export control regime, export control regulations, cyber security, control lists, export liability*

1. INTRODUCTION

The North Atlantic Treaty Organisation (NATO) created a political and military alliance between European and North American countries to provide for a collective defence alliance based on shared security concerns rooted in the common determination to protect the freedom, democracy, liberty and rule of law of member countries. In 1951, internal reports to the North Atlantic Military Committee reflected the concern that NATO's conventional forces had not met the requirements outlined to protect the NATO member states from a full-scale Soviet Union attack (NATO, 1951a; NATO, 1951b; Bitzinger, 1989). During that period, the United States (US) had reached a consensus with Britain and France to coordinate domestic export controls of strategic materials and technology that would prohibit specific goods from being exported to communist states and the multilateral coordination of domestic export controls was expanded to include other European countries as the restrictions were shown to be an important element in slowing down the technological advances that the Soviet Union gained from importing strategic goods (McDaniel,1993; Office of Technology Assessment, 1979). A separate international export control entity called the Coordinating Committee for Multilateral Export Controls (COCOM) was established to function as a collective means to wage economic warfare against the Soviet Union and the Soviet bloc. By 1985, all the member countries of NATO except Iceland were participating states of COCOM (McDaniel, 1993).

The structure of a modern export control regime was established through COCOM and consisted of multilateral negotiations done on an international level that would result in export control lists that countries would then have the discretion to adopt into their domestic export control regimes. COCOM had the strategic purpose of negotiating export control lists that would restrict military-use goods and technology from reaching the Soviet bloc, but it was established through a gentleman's agreement that did not give COCOM the ability to enforce the negotiated lists. The actual enforcement and implementation of export control lists were decided through domestic export control regulations and, in COCOM's early years, the US played a strong role in promoting the adoption of COCOM's export control lists into domestic export control regimes (McDaniel, 1993; Office of Technology Assessment, 1979). International export control agreements such as COCOM provided multilaterally negotiated export control lists and the domestic export control regimes offered different utilities that structured the elements of domestic export liability. Both are important in the discussion of export control regimes. The interplay of COCOM and domestic export control regulations worked together to create an added layer of economic policy consideration that worked to facilitate the collective defence for NATO member states.

The dissolution of the Soviet Union shifted the focus of NATO's security policy and also changed the purpose of international export control regimes. NATO went from being an organisation formed to provide collective defence against a common adversary to being an organisation that worked together

to build a system of collective security and interests. International political changes also affected the international export control regimes. As the export controls in COCOM were established for the specific purpose of containing conventional arms and dual-use goods and technology from reaching the Soviet Union, they were no longer necessary. COCOM was terminated in 1994 and replaced by the Wassenaar Arrangement (WA) in 1995. Instead of targeting specific countries for export control, WA created consensus among the participating states to establish control lists of conventional arms and dual-use goods and technology that would then be implemented in domestic export control regulations (Wassenaar Arrangement, 2019). The transition from COCOM to WA denoted a policy shift of international export control regimes that promoted regional and international security instead of being country-specific in its control list-making process.

The discussion of security concerns has expanded from traditional armed military threats to include online cyber security attacks, but the export control regimes were not constructed to easily adopt and reflect cyber security concerns. There are two reasons for this. First, the national security concern that is focal in export controls allows for governments to coordinate international and domestic export control regimes in a concentrated securities effort. In contrast, the widespread need for cyber security in both the private and public sectors makes the successful strategic planning of cyber security one that would need to be done through the coordination between the various industries. The feedback from the cyber security industry early in the policy-making process to address cyber security concerns would be more effective compared with the concentrated decision powers given to the government in the pursuit of national security considerations. Second, the regulatory construct for domestic export control regimes was established to restrict the cross-border movement of physical goods rather than the transmission of data and technology through the internet. Although domestic export control regulations have been amended to address the transmission of controlled technology through the internet, the two primary elements in the construct of domestic export control regulations have remained unchanged: 1) the control lists that decide what goods and technology are subject to export controls, and 2) the allocation of liability for regulatory compliance. Both of these elements were structured when the primary subject of export control was physical goods and as domestic export control regulations seek to incorporate cyber security into their export control, it is important to analyse and recognise why the construct of these two elements might not be the best structure to address cyber security concerns.

2. Challenges of Using Export Control Regimes to Deal with Cyber Security Challenges

Cyber security concerns pose challenges to the national security of countries, but to use the policy tools formulated under the traditional military-

oriented national security considerations might not help to address extant cyber security concerns. The formation of the strategic plans for national security concerns and cyber security concerns are fundamentally different. The former are driven by national governments and address a country's national security and tactical concerns. As export control regimes are viewed as trade measures rooted in military-oriented security considerations, the government acts as the main policymaker and enforcer of legislation that would restrict the export of military and dual-use goods and technology. The coordination of multilateral export control agreements such as WA and the implementation of these measures in domestic export control regimes reflect the government-centric approach of those regimes. The strategic planning of military-oriented national security concerns is concentrated at the governmental level and flows in a top-down manner where civil stakeholders have limited ability to respond unless invited by the government. Therefore, the formation of a national security strategic plan is different from the bottom-up strategic plan needed in cyber security strategy planning.

Although cyber security could be discussed as an extension of national security concerns, the definition of cyber security dictates that the creation of the strategic plans for it would be different from those of export controls. Craigen, Diakun-Thibault and Purse define cyber security as 'the organisation and collection of resources, processes and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights' (Craigen et al., 2014: p. 17). Another definition offered by the International Telecommunications Union (ITU) is: 'the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the availability, integrity and confidentiality of assets in the connected infrastructures pertaining to government, private organisations and citizens' (ITU, 2018: p. 13). Both definitions highlight the entities involved in dealing with cyber security strategic plans to be parties working from their respective industries in both the public and private sectors that have vested interest in being protected from cyber harm (ITU, 2018; OECD, 2012). The wide-ranging elements included in the definition of cyber security make it necessary for civil stakeholders from various industries to be involved in the strategic planning of cyber security to construct a policy that would address and reflect a wide array of issues that fall under the broad definition of cyber security concerns.

Besides the different ways that the governments and civil stakeholders interact with each other in their respective strategic planning process, another challenge for addressing cyber security concerns through the construct of export control regimes stems from the original subject matter of restriction under export control. Export control regimes were established with the focus of restricting the physical movement of goods rather than intangible technologies. Even for US Export Administration Regulations (EAR) that have incorporated knowledge-based export control measures, the determination of whether or not export licenses should be obtained

for controlled technology released to a foreign person was predicated on the exposure of controlled technology to the physical presence of a foreign person. As export control seeks to incorporate cyber security concerns into its regulatory framework, some of the primary elements of export control regimes that were not originally constructed to regulate the movement of software technology in cyberspace need to be reconsidered.

A. Interaction between Government and Civil Stakeholders

Modern export control regimes were established during the Cold War as an accompanying trade measure that reflected the security concerns of NATO regarding the looming threat from the Soviet Union to Europe and the outbreak of the Korean War in 1950. As governments implemented domestic regulations of export controls based on multilateral negotiations, the national security aspect of export control took priority over the potential economic sacrifices that civil stakeholders might have to bear. However, because the export control lists made during the COCOM era stemmed from these shared strategic concerns, the controlled goods and technology were conventional military-used or dual-use items that needed to be controlled based on their military orientation. The economic detriment that civil stakeholders encounter under export control regimes would be viewed by the government as necessary for the protection of national security.

To protect a country's national security, government agencies, especially the military, have also been a primary source of research grants in the research and development of advanced technologies (Singer, 2014). The internet itself would not have been created if not for the US Department of Defense funding the Defense Advanced Research Projects Agency (DARPA) that partnered with scientists, industry and academia to build the basic framework of the internet (Goldsmith and Wu, 2008; Singer, 2014). This creates an additional layer of proprietary control that governments might have towards the export of restricted military-use goods and technology. Even if the original funding for developing advanced technologies had been granted from government entities, the private sector finessed the use of these advanced technologies for broad commercial application and adopted them for general use. To control the export of technologies that have become commercially available even with specific national security needs, such as the export control of software that could generate cyber-attacks, would require feedback from the public and private sector as its use and proprietary nature are now shared among many stakeholders.

The traditional decision-making power in export control regimes has been centralised in the government and resulted in a top-down flow of requests for regulatory compliance for civil stakeholders. As a result, the participating states of the multilaterally negotiated international export control lists from COCOM and current international export control agreements that include WA, the Missile Technology Control Regime, the Nuclear Suppliers Group and the Australia Group would be adopted into the US and EU dual-use export control lists without seeking comments or feedback from the general

public. Divergence from this general practice happened in the US when cyber security software, specifically intrusion software and surveillance items, were added to the WA export control list after the 2013 Plenary Meeting. The different methods that the US Department of Commerce and EU responded to the WA 2013 Plenary Meeting Agreement reflected the different perspectives that governments have in incorporating cyber security considerations into export control regimes.

For the EU, the use of export controls to promote security has become inclusive of protecting human rights as a human security focus. There was an amendment made to EU's dual-use list in 2014 to include WA 2013 Plenary Meeting Agreement's control of intrusion software and Internet Protocol (IP) network communications surveillance system or equipment (European Commission, 2014). The export control of intrusion software and surveillance items was deemed to be necessary as these technologies had allegedly been used by autocratic states to monitor and arrest dissidents (Kanetake, 2019). Because the construct of export controls was based on protecting the security of the exporting country defined by the government, as the EU incorporates the value of protection of human rights as a security concern.

In an administrative move usually not seen when implementing the agreed export control list, the US Department of Commerce posted the proposed rules and sought comments for implementing the WA 2013 Plenary Meeting Agreement (BIS, 2015). There was concern from the Department that the scope of export control over intrusion software would be too broad and that public feedback would be needed to make sure that the rule would not harm the US government or cyber security industry within the private sector if it was implemented. When the then Assistant Secretary of Commerce for Export Administration Kevin J. Wolf testified before the US Congress in 2016, he acknowledged that the public response was mostly negative rules (BIS, 2016). The initial inquiries for the proposed rule reflected a different understanding of the terminology used in the control list entries by the cyber security community than by the export control agencies and the WA participating states and commenters also worried that the measures could not be implemented without causing significant harm to cyber security. As a result, even though intrusion software and surveillance technology remained on WA's export control lists, the US has yet to adopt these restrictions.

Export control regimes were constructed with a policy focus on national security that allowed governments to exert control over the subject matter of the controlled items and technology, but the way that dual-use technologies have evolved to widespread public and private sector use might make future export control rule-making something that would need more private sector input. This underlying tension is seen in the way the main elements of export controls have been structured.

B. Primary Elements of Export Control

Adding classes of cyber security technology into export control lists seems

like a natural extension of the use of export control regimes since their main policy goals are to restrict the export of technologies that would result in military and/or cyber attacks to the exporting country. However, the construct of export control regimes creates friction with some of the policy concepts of cyber security and has resulted in export control being less effective in promoting cyber security. The two primary elements that construct export control regimes have remained unchanged even with the arrival of the internet: 1) the control lists that decide what goods and technology are subject to export controls; and 2) the allocation of liability for regulatory compliance.

These aspects have served to create cohesion among the domestic export control regulations between nations, but adopting them for cyber security has showcased the inherent weakness. The foundational construct of export controls is the use of bans and restrictions, but this construct is not found in the methodology for constructing cyber security strategies in most countries. Cyber security strategies require the involvement of civil stakeholders. The fundamental construct of cyber security is the co-operation between stakeholders in formulating measures to diminish cyber security risks and fend off attacks (Public Safety Canada, 2019; US Department of Homeland Security, 2018; US Department of Commerce, 2017; Klimburg, 2012). The use of export controls requires policymakers and stakeholders to narrow the focus to debating what types of information technology and what specific software and technologies should be restricted or banned for export instead of taking an overview of cyber security strategies from a cooperative approach between government and stakeholders. This creates a concentrated focus on determining what information technology should or should not be subject to export controls while being mindful of the liability that might be imposed on parties that violated export control regulations. The following sections will break down the two foundational elements in export control regulations to address the two issues: why identifying technology to add to control lists might not be effective for cyber security tactics, and why the methods used to allocate export control liability are not helpful in addressing cyber security concerns.

1) Control Lists

After World War II, international export control regimes such as COCOM and WA facilitated multilateral negotiations among participating states so that the states could adopt similar control lists and create unity in controlling the movement of goods and technologies. The lists provided a framework for the construction of domestic export control regimes. Even though countries have the ultimate decision-making power of incorporating the control lists into their domestic export control regimes, most adopted the control lists from the international regimes thus forming a cohesive international approach.

Adding technology as an intangible subject of control into control lists thus far made up only of physical goods was much debated in the early 1980s. Many COCOM member countries opposed such an addition, as it would be difficult

to enforce export controls over the intangible forms of data and technology (McDaniel, 1993). The difficulty of enforcement lies not only in the intangible nature of data and technology, but also in determining whether or not it belongs to a category on the control lists. A cargo box sitting in a port might contain export-controlled items that require an export license, but whatever physical item is in the cargo can be categorically determined. A review of the questions submitted for the United States Department of Commerce, Bureau of Industry and Security (BIS)'s proposed rule for WA plenary agreements highlights the technological complexity and actions that are taken to create a cyber security ecosystem. Policymakers need to identify specific technologies, systems or tools that are part of that ecosystem and label them as subject to export control when they bring cyber security into the construct of an export control regime. Within the vast scope of software and technologies that build the cyber security ecosystem, trying to separate particular technologies and systems for export control does ignore the interwoven connections of a cyber security strategy framework. Therefore, while it is possible to address cyber security concerns through adding specific software or technology to export control lists, the purpose of control lists and the general construct of a cyber security ecosystem would not make the use of export control lists the best method of addressing cyber security concerns.

2) Export Liability

The construct of domestic export control regimes is determined by the establishment of control lists and the allocation of export control liability. Historically speaking, the establishment of control lists was organised through multilateral efforts under international export control regimes and the allocation of liability determined through domestic regulation. Allocating export liability identifies the party responsible for ensuring that all export activities are conducted in compliance with domestic export control regulations. While there are differences between each country's regulations, two definitions are generally found that help construct the liability framework: the exporter who is liable for export control compliance and the export activity that triggers that control.

Export liability is generally allocated to exporters because they have the control and decision-making power to send items or transmit technology abroad. In some jurisdictions, exporter's liability is imposed because there is a presumption that they will receive financial gain from the export activity. In the case of US, EAR Part 772 defined exporter as '[t]he person in the United States who has the authority of a principal party in interest to determine and control the sending of items out of the United States' (Bureau of Industry and Security, 2020: p. 16). EAR Part 772 also describes the principle parties to be 'persons in a transaction that receive the primary benefit, monetary or otherwise, of the transaction. Generally, the principals in a transaction are the seller and the buyer' (ibid.) This is similar to the definition in EU Council Regulation (EC) No. 428/2009 Article 2 where an exporter is a person who:

> ‘holds the contract with the consignee in the third country and has the power for determining the sending of the item out of the customs territory of the Community ... [However] [i]f no export contract has been concluded or if the holder of the contract does not act on its own behalf, the exporter shall mean the person who has the power for determining the sending of the item out of the customs territory of the Community... [or] transmit or make available software or technology by electronic media including by fax, telephone, electronic mail or by any other electronic means to a destination outside the Community’ (European Council, 2009: p. 2).

The subtle difference in the definition of exporters could affect the allocation of export liability for actors in cyberspace, especially as it relates to the liability of platform services. For example, in an Advisory Opinion issued in 2009, BIS determined that online cloud computing storage services would not be considered to be an export under EAR because they are not considered to be a party of interest. The party of interest was the user of the service (BIS, 2009). The same issue of using online cloud computing services might result in a different interpretation under EU Council Regulation (EC) No. 428/2009 since the definition of an exporter is not tied to the entity receiving economic benefit for their actions. The exporter is the person that sends items outside of the export control jurisdiction and is responsible for export control violations, but identifying the exporter in cyberspace might not be as straightforward as it is with identifying the exporter that ship goods in the physical world.

For the exporter to be held liable, an export activity must happen to trigger export liability or a broader export liability could also be imposed on exporters that fail to secure the protected items. The general definition of export is when goods or technologies are sent or transmitted across borders and so the transmission of data and software through cyberspace is subject to export control if it is clear that it has crossed a border. However, in some countries like the US, an export activity is not restricted to the traditional cross-border movement of goods and technology. Allowing a foreign person to gain knowledge of export-controlled technology inside the US is also prohibited as an act of ‘deemed export’ which under the US EAR is defined as the release or transfer of technology to a foreign person inside the US. The concept of export activities under this definition is therefore focused on the exposure of knowledge rather than the movement of allowance of goods and technology between sovereign jurisdictions.

The liability framework was originally constructed with the idea that the person who was responsible for sending the goods intends that they cross a border. However, with the advent of the internet, the relationship between the parties involved with the transmission of technology and data might not fit the traditional definitions of exporter and export activities. Consideration

should be given to whether the framework established to regulate the movement of goods should automatically be adopted to address new national security concerns such as cyber security. Internet service providers (ISPs) and online storage companies act as agents for transmitting or storing data on the internet, but they have been mostly excluded from export control liabilities. This is because ISP users, not ISPs, are considered to be exporters as they are the 'principle party in interest' under US EAR and the entity receiving economic benefit under EU Council Regulation (EC) No. 428/2009. As ISPs are parties that could contribute most to cyber security planning, the exclusion given to ISPs might not be the best construct to protect against cyber security threats.

3. Refocusing Export Control Regimes to Address Cyber Security Concerns

As technology has advanced, export control regimes must evolve to reflect the new reality of the transfer of data rather than physical goods. Changes thus far have not shifted the foundational construct of using control lists to allocate export liability to the exporter of controlled items or technology. This creates tension between government and civil stakeholders and makes it difficult to achieve cyber security policy protection through the construct of export controls. Change is needed to decrease the friction between civil stakeholders and government entities when incorporating cyber security concerns into export controls. Like-minded NATO countries should work together to build a public-private partnership based on voluntary cooperation between government agencies and civil stakeholders in order to address cyber security concerns.

A proposed change is needed to find a way to address these issues which should see the involvement of civil stakeholders in the construct of these lists. Current export control lists identify goods and technology that could endanger national security. A control list acts as a prohibitive measure that details the goods and technologies that should not be exported, so instead of focusing the control lists on software or technology that would be harmful to national security, another type of list could also be established specifically to provide for information security, network security and operational security as they relate to the software and tools that would be helpful in building a cohesive cyber security framework among participating states. It is important in the construction of this new list that input from cyber security industry and experts be incorporated from the start and instead of creating liability for the technologies listed in cyber security items, an exemption would be given to the cross-border movement of items on this list among member states that are building a common cyber security framework. The goal is to build more cooperation between civil stakeholders and various national governments to maximise efforts to promote cyber security between different states.

4. CONCLUSION

NATO was created as a political and military alliance between European states and North American countries to provide for a collective defence alliance based on shared security concerns rooted in the common value of protecting the freedom, democracy, liberty and rule of law of member countries. It is through these shared security concerns that modern export control regimes have been established. While the use of export control regimes to resolve cyber security threats could be discussed as an extension of national security considerations, the formation of strategic plans for national security concerns and cyber security concerns is fundamentally different. There is a need to reconsider how cyber security issues could be incorporated into the export control regime framework through a list-building process that could promote closer working relationships between member states that share similar security concerns.

5. REFERENCES

Bitzinger, R.A. (1989) *Assessing the Conventional Balance in Europe*, 1945-1975, Santa Monica, the RAND Corporation.

Bromley, M., Cooper, N. & Holtom, P. (2012) The UN Arms Trade Treaty: Arms Export Controls, the Human Security Agenda and the Lessons of History. *International Affairs*. 88 (5), 1029-1048.

Bureau of Industry and Security. (2009) *Application of EAR to Grid and Cloud Computing Services*. Available from: https://www.bis.doc.gov/index.php/documents/advisory-opinions/527-application-of-ear-to-grid-and-cloud-computing-services [Accessed 14th August 2020].

Bureau of Industry and Security. (2015) Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items, *Federal Register* 80, 28853-28863. Available from: https://www.federalregister.gov/documents/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items [Accessed 14th August 2020].

Bureau of Industry and Security. (2016) *Testimony by Assistant Secretary of Commerce for Export Administration Kevin J. Wolf Before the House Committee on Oversight and Government Reform, Subcommittee on Information Technology and the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies on 'Wassenaar: Cybersecurity and Export Control'.* Available from: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/1393-doc-testimony-for-asst-sec-kevin-wolf-1-12-16/file [Accessed 19th September 2020].

Bureau of Industry and Security. (2018) Review of Controls for Certain Emerging Technologies, *Federal Register* 83, 58201- 58202. Available from: https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies [Accessed 14th August 2020].

Bureau of Industry and Security. (2020) Export Administration Regulations Part 772: Definition of Terms. Available from: https://www.bis.doc.gov/index.php/documents/regulations-docs/2344-part-772-definitions-of-terms-2/file

[Accessed 21th November 2020].

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014) Defining Cybersecurity. *Technology Innovation Management Review.* 4 (10), 13-21. Available from: doi:10.22215/timreview/835.

European Council. (2009). *Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items*. Available from: https://eur-lex.europa.eu/eli/reg/2009/428/oj [Accessed 25th November].

Goldsmith, J. & Wu, T. (2008) *Who Controls the Internet?: Illusions of a Borderless World*. New York, Oxford University Press.

International Telecommunications Union. (2018) *Guide to Developing a National Cybersecurity Strategy*. Available from: https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018 [Accessed 14th August 2020].

Kanetake, M. (2019) The EU's dual-use export control and human rights risks: the case of cyber surveillance technology, *Europe and the World: A law review*. 3 (1). Available from: doi:10.14324/111.444.ewlj.2019.14.

Klimburg, A. (Ed.) (2012) *National Cyber Security Framework Manual*, NATO. Available from: https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/ [Accessed 14th August 2020].

McDaniel, D.E. (1993) *United States Technology Export Control*. Westport, Praeger Publisher.

NATO. (1951) *Item MC 0031-Final-Readiness and Effectiveness of NATO Forces*. Available from: https://archives.nato.int/readiness-and-effectiveness-of-nato-forces-2 [Accessed 19th September 2020].

NATO. (1951) *Item MC 0033-Final-Estimate of the Relative Strength and Capabilities of NATO and Soviet Bloc Forces at Present and in the Immediate Future.* Available from: https://archives.nato.int/estimate-of-relative-strength-and-capabilities-of-nato-and-soviet-bloc-forces-at-present-and-in-immediate-future [Accessed 19th September 2020].

National Institute of Standards and Technology. (NIST) (2018) *Framework for Improving Critical Infrastructure Cybersecurity.* Available from: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 [Accessed 14th August 2020].

Office of Technology Assessment. (1979) *Technology and East-West Trade.* Washington, D.C., Office of Technology Assessment Publications.

Organisation for Economic Co-operation and Development (OECD). (2012) *Cyber Security Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the Internet economy.* Available from: https://www.oecd.org/sti/ieconomy/comparativeanalysisofnationalcybersecuritystrategies.htm [Accessed 14th August 2020].

Public Safety Canada. (2019) *National Cyber Security Action Plan 2019-2024*. Available from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx [Accessed 14th August 2020].

Public Safety Canada. (2018) *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. Available from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx [Accessed 14th August 2020].

Ruohonen, J. & Kimppa, K.K. (2019) Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software and Ambiguity. *Journal of Information*

Technology & Politics. 16 (2), 169-186.

Singer, P. (2014) *Federally Supported Innovations: 22 Examples of Major Technology Advances That Stem from Federal Research Support*. Washington, D.C., The Information Technology & Innovation Foundation.

US Department of Commerce. (2017) *International Cybersecurity Priorities: Fostering Cybersecurity Innovation Globally*. Available from: https://www.commerce.gov/news/reports/2018/06/international-cybersecurity-priorities-fostering-cybersecurity-innovation [Accessed 14th August 2020].

US Department of Homeland Security. (2018) *Cybersecurity Strategy*. Available from: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf [Accessed 14th August 2020].

Wassenaar Arrangement. (2014) *The Wassenaar Arrangement on Export Control for Conventional Arms and Dual-Use Goods and Technology: List of Dual-Use Goods and Technology and Munitions List.* Available from: https://www.wassenaar.org/app/uploads/2019/consolidated/WA-LIST-14-2.pdf [Accessed 14th August 2020].

Wassenaar Arrangement, Public Documents. (2019) *Vol. IV – Background Documents and Plenary-related and Other Statements.* Available from: https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-PUB-006-Public-Docs-Vol-IV-Background-Docs-and-Plenary-related-and-other-Statements-Dec.-2019.pdf [Accessed 14th August 2020].

The Challenge of Networked Complexity to NATO's Digital Security

Laurin B. Weissinger
Lecturer
The Fletcher School
Tufts University

Abstract: In the aftermath of the 2016 Democratic National Convention (DNC) hack and with ongoing disinformation campaigns attacking democratic elections worldwide, cyber defence has never been more important for the North Atlantic Treaty Organisation (NATO) allies. However, current security strategies often fall short because they do not adequately address the problem of networked complexity. To protect cyberspace, national assets and key institutions, we must solve for the strategic, tactical and operational complexities of the technology stack, including its interconnections and interdependencies.

States and organisations must address three levels of complexity: entity, layered and networked complexity. Entity complexity is the complexity of a single component or system, for example, a central processing unit (CPU). Layered complexity arises when we layer multiple levels of complex hardware and software. The third level of complexity involves emergent networks and interactions of multi-layered technical and socio-technical systems.

This paper establishes the critical importance of understanding networked complexity in cyber security, a topic which is underrepresented in extant cyber security literature. It proposes practical solutions, including a focus on 'defence in breadth'. All systems, including consumer-grade products, must be shipped more secure by default. Mitigating networked complexity in cyber defence will also require better threat and attack modelling. Security strategies should move from hierarchical models to a graph-driven, networked understanding of cyber security that incorporates socio-technical dimensions. Lastly, states should leverage the security community and public-private partnerships.

Keywords: *Networks, complexity, national security, defence, cyber security*

1. INTRODUCTION

Today's world is digital, complex and networked; security must address that. Internet outages, cyber criminality like ransomware (Mathews, 2017; Conolly & Wall, 2019) and information operations like the DNC hack have already caused considerable damage (Nakashima, 2016; Taub, 2016). Western democracies are particularly vulnerable among digitised states due to how their societies and economies are organised. Free markets, individual liberties, free enterprise and open societies (Popper, 2013) foster complex network of ties rather than limiting actors to top-down relationships.

Socio-technical systems and 'information networks' (Castells, 1996; Castells, 2000; Castells, 2001) in their interconnected entirety constitute the basis and fabric of our society, making society and economy in Western democracies highly interdependent:

> A network society is a society where the key social structures and activities are organised around electronically processed information networks ... It's about social networks which process and manage information and are using micro-electronic based technologies ... The global economy is based on the ability of the core activities—meaning money, capital markets, production systems, management systems, information—to work as a unit in real-time on a planetary scale. [This] increases the complexity, the size and, ultimately, the volatility of global financial markets (Castells, 2001).

This paper explores networked complexity and the global cyber security risks that emerge when computer systems (comprising layers of complex components themselves) are connected across organisations and used to run crucial and complex social, bureaucratic and economic processes. The vulnerabilities described in this paper will only intensify with increasing, widespread use of oftentimes insecure (Singh et al., 2016) IoT devices, more industrial control systems and growing reliance on IT systems overall. Since 2007, more 'things' than people have been using the internet (Evans, 2011). Unless states develop a 'security in breadth' approach, these cyber security risks threaten the very existence of open societies and the democratic freedoms championed by NATO allies.

The paper explains how networked complexity threatens cyber security and how states and organisations can mitigate the dangers and solve for the challenges posed by networked complexity. The first section provides foundational framing for understanding interdependence and complexity. The second elucidates why interdependence and complexity are critical for contemporary cyber security. The final section proposes practical policy solutions.

2. HISTORY AND TYPES OF COMPLEXITY

This section describes how systemic interdependence and resulting complexity have developed alongside the evolution of technology and society over the last 150 years and categorises different tiers of this phenomenon. Emile Durkheim (1893), a scholar of modernity, conceptualised the increasingly specialising, interdependent structure of then-contemporary society in the late 19th century as 'organic'. Through specialisation, distinctive technology and mastery, experts become individually so productive that even groups of untrained individuals cannot match them. Society and its members specialise and optimise under organic conditions, relying on each other like organs in a body. This process creates ties and dependencies all across society.

Thus, each specialist becomes dependent on other social 'organs' to perform their own function. For example, contemporary agriculture in developed countries is a high-yield, high-tech enterprise, using drones, sensing technologies, and data mining (Meola, 2016; NIFA, 2020). Food production has become more effective and efficient, but farmers are now reliant on various specialist providers of niche technologies (Cyber Risk, 2020) that they require but cannot themselves produce.

Computers consist of interacting, complex and specialised hardware and software components and are built around similar ideas as Durkheim's organic society. This paper posits three levels of complexity (Table I) that apply to technical, social and socio-technical systems: entity complexity, layered complexity and networked complexity.

Table I: Types of Complexity

	Entity Complexity	Layered Complexity	Networked Complexity
Dimensions	Component/ Node	One-dimensional ties/dependencies	Multidimensional networks of ties/ dependencies
Ties / Dependencies	N/A (excludes manufacturing)	ties = $n^{components} - 1$	ties = $n^{components} * (n^{components} - 1)/2$
Dependency Types	N/A	Uni-directional	Multi-directional, interactive
Example	Random Access Memory Module	OS running inside virtual machine	Computer network used by organisation

Entity complexity speaks to the complexity or intricacy of a single component. For example, modern, general purpose operating systems are based on millions of lines of code written by multiple teams of engineers, under varying situational and procedural entanglements (Clarke et al, 2016). They are designed to function with different sets of hardware and software and in various circumstances. Truly grasping them as a whole, as Fathi's (2018)

account of the development of Windows Vista shows us, is nearly impossible. Correspondingly, many specialised professions, complete with their particular lexicons, cannot be easily grasped by outsiders due to their intricacy.

Layered complexity is the outcome of vertical dependencies, like running specialised applications on operating systems which can run virtually using a hypervisor that hands instruction down to the CPU. Similarly, in value chains, many business models and products rely on already complex products or services that they build on top of and cannot function without, for example, digital communications or developed road and rail networks.

This paper predominantly focuses on the third level: networked complexity. A multitude of interdependencies is a reality for both social and computer systems. Computer systems and value chains are not monolithic or simply layered, but rather an assortment of networked components (Mahutga, 2012). Analytically, such socio-technical systems present themselves as intricate and not always intelligible, webs of interdependencies, which is why networked complexity and the resulting security risks warrant particular attention. While some nodes and ties may be more important than others and some hierarchies exist, most of the relationships are necessary, or at least beneficial, to the overall functioning of a system. For example, software requires the hardware layers and most hardware is ineffectual alone—only complete systems function.

In this context, a 'system' is an entity or network that has a social function and includes all components necessary for operation. Some computer components, like graphics adapters, are essentially computers in their own right, but they cannot operate on their own. Similarly, a group of individuals with one social function, e.g. the production of goods, is a social system. For a manufacturing company, the IT department would be a subsystem or component; it is necessary but not sufficient for production.

Complex, networked systems are difficult to understand and predict while demonstrating emergent properties (Goldstein, 2011): different agents and subsystems interact and together create systemic evolution. This is why replicating complex (production) networks remains problematic for high technology like contemporary military systems (Gilli & Gilli, 2019). Accumulated, uncoordinated decisions on a micro level can effect macroscopic change (Schelling, 2006). The more functions, variables and relationships a system needs to manage, the more likely it becomes that unexpected events will occur and errors, inconsistencies and inefficiencies will be missed.

Even within components, networked complexity can exist: the philosophy of Unix, the system that inspired contemporary operating systems, is to create small programs that are extremely effective and efficient at doing one specific task and to make those specialist programs interact (Kernighan & Pike, 1984). Using and networking building blocks remains best practice in contemporary software development. System architects usually buy

standard hardware from expert manufacturers and use a proven operating system, relying on someone else's network and protocol implementations. Then they build upon an established database like MariaDB and packages like OpenSSL for encryption. Finally, software is written in higher-level programming languages designed by others. Only in outlying cases where existing building blocks are insufficient would one use lower-level code like Assembler or build specialised hardware. This adds additional complexity and vulnerabilities: many satellites rely on old, space-optimised, weight-and-power-limited computers that thus lack basic security features (Eddy, 2019).

To properly function, all systems and organisations require resources they often cannot provide, produce, or even fully understand (Hirsch, Fiss & Hoel-Green, 2009). In such complex systems, non-complex and complex errors and vulnerabilities emerge. The latter may be unpredictable or inconsistent in their macro-level effects (Schelling, 2006). This paper focuses on addressing the security issues that arise when we take many inherently intricate, niche-expertise-based products and connect them all into large and heavily interdependent networks that consistently cross the socio-technical divide.

3. How Networked Complexity Shapes the Security Environment

Organic interdependence and specialisation allow for considerable improvements in productivity, speed and quality in computing (Dally et al., 2020) and in society (Krugman, 1980; 1981). The same networked complexities and dependencies produce unintended and unwanted security vulnerabilities. This section explains how complexity shapes the security environment, how dependencies both increase and decrease security risks and how complex and non-complex errors and vulnerabilities arise.

As Table I shows, a complete security analysis of a networked system quickly becomes impossible. Each added node or subsystem can significantly increase dependencies and interactions that would have to be modelled, analysed and proven to be secure.

Nevertheless, 'outsourcing' security often results in a clear net benefit if not overdone (Schneier, 2002). Expert providers can leverage specialisation to provide better and otherwise unavailable security products and services. Thanks to specialisation and economies of scale, smaller organisations and non-experts can improve their security by relying on specialised outlets with more experience, expertise and skill. For example, most organisations would see security increase when moving their email to a hosted solution by Google or Microsoft, or by relying on specialist authentication providers like Duo. The security of key components, like operating systems, has also improved considerably in recent years.

This does not mean it is impossible for small organisations to run secure systems. Rather, relying on outside expertise is likely to yield better results because specialists can provide a niche product or service to multiple customers at an individually lower cost. This optimisation of security cost/benefit ratios occurs at all levels: NATO's militaries and multinational firms do not provide all IT services internally or build all their equipment themselves; like other organisations, they acquire resources from specialists (defense.gov, 2020).

While this specialist-led approach can reduce vulnerabilities per product or service, it increases networked complexity and dependencies. When connecting to and relying on immense numbers of providers, systems and hardware/software stacks, the universe of cases, including the potential states, situations, dependencies, interactions, attack vectors, vulnerabilities and risks grows immensely. It is common practice in research and analysis to limit the inquiry to a manageable number of cases and variables (Nielsen, 2016). However, in our networked world, it becomes difficult organisationally and technically to retain security perimeters, to track what is needed to run processes, or to identify which of the many relationships or data flows are legitimate (Vijayan, 2013). For example, organisations often struggle to block malware and phishing sites hosted on large, legitimate cloud services, as these services see sufficient use to be allow-listed (Nelson, 2016).

The 'seams', that is the interactions between systems rather than individual systems themselves, are a key security concern when connecting organisations (Schneier, 2003). Organisations often cannot interface easily because they have divergent needs and processes; in effect, they speak different languages. Furthermore, seeing the interface between two organisations as a dyadic relationship is oversimplified. Different, potentially insecure, social and technical systems might have to be tied together to acquire the required resources. For national cyber security, these issues are exacerbated: networked complexity increases exponentially with the width of our analysis parameters, creating emergent properties and hard-to-trace dependencies and interactions.

Complex systems can produce both complex and non-complex errors. The latter are consistent, while the former is indeterminate or emergent. It is extremely difficult to test complex entities exhaustively, particularly under networked conditions where interactions affect how vulnerabilities present themselves. Complex vulnerabilities in hardware and software may only arise in outlying cases and be triggered only by specific circumstances and can thus remain undiscovered for years. The Heartbleed vulnerability in OpenSSL only manifested itself in some versions of the package and was disclosed two years after the implementation of the vulnerable 'heartbeat' feature (Durumeric et al., 2014). More drastically, the Spectre and Meltdown vulnerabilities found in 2018 affected thousands of microprocessors that 'implement out-of-order execution' (Meltdownattack.com, 2020). Spectre and Meltdown remained undetected for many years and had different effects

depending on the affected system—a prime example of how complexity can create security risks.

Complex systems can also create non-complex errors: in the case of the Intel FDIV bug, the affected processors produced errors when dividing numbers (Price, 1995). The bug was discovered within a year and Intel replaced the affected units. The Intel F00F bug from 1997 was also predictable and consistent; certain instructions would cause the CPU to 'hang up'. Software workarounds were created and deployed, resolving the issue (Collins, 1998). The FDIV and F00F errors were non-complex errors in a complex system: they were rather obvious and, most importantly, consistent. Spectre and Meltdown, by contrast, constitute complex errors. Hidden in the complexities of branch prediction and out-of-order execution, these vulnerabilities are less obvious and produce inconsistent outcomes depending on processor type and applications. Currently, it is only possible to harden systems against the exploitation of Spectre; the vulnerability is not fixed (Meltdownattack.com, 2020).

While these bugs and vulnerabilities are predominantly technical in nature, the political economy of security was part of the reason why the Heartbleed vulnerability was overlooked: the OpenSSL project was painfully underfunded and understaffed. Multi-million-dollar companies and essentially the entire internet user base relied on a few volunteers, as John Walsh (2014) outlined:

> OpenSSL … is largely staffed by one full-time developer and a number of part-time volunteer developers. The total labor pool for OpenSSL maybe adds up to two full-time developers. Think about it, OpenSSL only has two people to write, maintain, test and review 500,000 lines of business-critical code. Half of these developers have other things to do.

Complex errors are not only present in cyber security but also appear in other complex systems and across socio-technical divides. The Boeing 737 MAX jets' fatal flaw was also a result of socio-technical networked complexity. The interaction of control systems, sensors, the fuselage design, management pressure, economic incentives, lack of functional regulatory oversight and the culture change created by the Boeing McDonald Douglas merger, all had their inter-related impact on a plane that cost over 300 people their lives (Sgobba, 2019; Herkert et al., 2020).

The examples above demonstrate different complexity-related issues: some errors like the FDIV and F00F are borne out of complex systems but could be identified and addressed easily. Complex systems, however, can also produce complex errors that are situation-specific and hard to predict or fix, as demonstrated by Heartbleed and Spectre/Meltdown. The Heartbleed and the Boeing 737 MAX examples also show how socio-technical interactions can cause literally and metaphorically fatal failures across domains.

Standardisation and strict operating protocols such as in air traffic and railways safety and control have long been tools to reduce complexity, counteract emergence and reduce failure rates (Vaughan, 2005; Hutter, 2001). In cyber security, however, this approach of codifying behaviour, unifying equipment and separating duties is less effective and therefore not the focus of this paper. First, computer and social systems diverge to an extent that makes complete standardisation impossible. Second, safety has very different objectives than security. Third, safety deals with trained, benevolent professionals rather than creative, malicious adversaries.

Security must also be analysed differently, specifically covering socio-technical networks, as evidenced by the DNC hack. Political parties and their leadership are at risk because they are closely tied to the core institutions of democracy, fundamental governance and societal aspects of most NATO members. Compromising a political party's leadership can disrupt the heart of a country's political system. Adversaries do not have to change election results. Sowing distrust and suspicion can be enough to blemish the central democratic institution in popular perceptions. Thus, less direct and more clandestine and socially-focused operations are an important vector to study (Hansen & Lim, 2019). Generally speaking, the old perimeter logic hardly applies anymore: compromises through others, be they employees' private devices or business partners' systems, are likely, particularly when dedicated adversaries—state or otherwise—are involved.

4. POLICY, TREATMENTS AND SOLUTIONS

For NATO countries and other open societies, networked complexity means that weaknesses within and attacks via the cyber realm are hard to analyse and predict. National and international interdependencies are so numerous and intricate that tracing and treating all security-relevant dependencies, attack paths and resulting risks is unrealistic. Adversaries, criminal and state-sponsored, have manifold options to compromise, disturb or otherwise undermine technical and social processes and key institutions. This section proposes solutions to reduce the attack surface and mitigate security issues borne out of interdependence and complexity.

While no one can eliminate the risk inherent in linking with other organisations or in running complex organisations and systems, mitigation is workable and can be effective. Security management measures can avoid or reduce the risk of an adverse event or incident taking place, or alleviate its detrimental impacts. The goal for organisations and governments should not be to create perfect security systems but instead to make compromising systems harder for adversaries to infiltrate and attack at every stage.

A. Security Management

The challenge of interlinked systems and complex dependencies calls for

more attention than currently warranted. Information security risk management processes have long addressed and dealt with dependencies and different attack paths. With growing complexity, however, existing methodologies, registers and models are more difficult to deploy and thus more expensive and failure-prone.

Now more than ever, organisations require numerous sets of niche knowledge and skills working in tandem to address security, which specifically entails technical and non-technical experts. These teams also need considerable time and resources to design, grasp, secure and maintain computer systems in their procedural and organisational contexts (Clarke et al, 2016). More time and effort must be dedicated to holistically analysing potential attack vectors and the security and trustworthiness of partners and suppliers.

In particular, analyses must incorporate socio-technical interactions, not just social or technical levels on their own. While labour-intensive, tracking and categorising ties and dependencies alongside what they entail can inform security policy, strategy and tactics and identify key nodes or ties requiring additional controls. While post-facto security is often less effective than building 'secure by design', the approach still reduces risk and is sometimes unavoidable, particularly when legacy systems are involved.

This holistic approach will be a multi-pronged challenge for many security professionals, who are often technical specialists (Weissinger, 2018). Few have cross-domain expertise, though this is changing. Additionally, non-technical personnel are often considered inferior or irrelevant by those within technical circles (ibid.). Lastly, individual time and bandwidth are limited: security specialists cannot be experts in everything and thus must cooperate and usually are not trained to do so (ibid.).

IT security management literature and standards like the ISO 27000 (2018) family and NIST 800-53 (2020) also underscore the importance of good security and risk management. Unfortunately, aptly implementing these high-level standards requires expertise, time, resources and, most of all, the will to improve security. With audits and certifications, experts often lament the tendency to demote security to 'box-ticking' exercises and the at times circumspect independence of auditors (Weissinger, 2018). Nevertheless, the Payment Card Industry Data Security Standard (PCI DSS) is a good example of useful standard enforcement. Whilst it did not lead to enhanced security everywhere, its mandatory nature did force payment processing companies to take security precautions (Wilson et al., 2018).

Crucially, security management can only reduce, not eliminate, risk (Purser, 2004) and, unfortunately, digitally securing a state is obviously far more elaborate, particularly when societies and economies are diverse, open, interlinked and interdependent (Castells, 1996; Castells, 2000).

B. Using Expertise Securely

Specialist organisations can bring non-specialists up to speed and also pro-

duce security that is of better quality and available more quickly. The greater the number of organisations that rely on them, the more likely it is that key security providers will become sought-after targets. However, shifting responsibility towards specialist providers and manufacturers is rational; very few actors have the ability to adequately address sophisticated threat actors.

To leverage expertise through layering and networks, three conditions must be at least partially met. First, individual components (technical and organisational) need to and need to be forced to, follow security best practices, particularly for components that are essential due to their stack position or layer, such as CPUs and operating systems. Second, ties or interconnections between layers and across networks must be established and maintained securely. Finally, any organisation relying on external providers and manufacturers must strictly monitor those relationships. Thus, we require more efficient and effective methodologies and approaches to assess the trustworthiness of service providers (Weissinger, 2017; Weissinger, 2018).

C. Secure by Design

To manage security risks stemming from increasing complexity and dependency on outside parties, system architects and managers should build towards greater resilience. For critical systems that must not be compromised, the best solutions are often not technical but architectural. For example, France's media blackout prior to its elections helped foil a Russian interference campaign in 2017 (Vilmer, 2018). 'Old-fashioned' low-tech or no-tech safeguards can also be resurrected, like paper trails being used to help secure elections.

To increase resilience across society, components—that is, products and services—must become more secure by default, based on an approach this paper terms 'defence in breadth', in addition to defence in depth. Defence in breadth means that security is designed into products and services, including consumer-oriented ones.

Agencies and key businesses matter profoundly to national security and they in turn are staffed by individuals relying on consumer products. While targeted security improvements are necessary, they are insufficient to fully manage networked security risks. Focusing security efforts only on key government institutions or critical infrastructure—however defined—leaves adversaries with a multitude of easily attackable devices, people and organisations through which they can compromise key targets indirectly. Furthermore, as evidenced by the DNC example, criticality has often been defined in an overly limited manner.

Defence in breadth can be supported by security research similar to Google's 'Project Zero' (2020) that focuses on often-used, essential technologies. More importantly, however, organisations and governments should make security baselines like secure defaults, basic penetration tests, security and data management audits, patching infrastructure and monitoring, manda-

tory across the board.

D. Specific Actions: Organisations
Individual organisations and agencies need to accept that networked complexity and its resulting risks, require managing. Networked complexity is hard to address with 'checkbox compliance' and with checks on building blocks alone. Therefore, socio-technical, network-based analyses must be added to conventional or routine security operations. Proper security management structures must be established. Specifically, individual organisations should trace key networks and create detailed dependency charts (Schostak, 2018; Schostak, 2014; Wheeler, 2011).

Most importantly, best practices like risk management, business continuity and disaster recovery planning should be followed and regularly audited. Particularly, organisations should think about backup solutions in the broadest sense such as planning for security failures in partner organisations.

E. Specific Actions: NATO and Governments
Grappling with the complexity of digital systems will require a division of labour within NATO, across state borders and across the public/private divide. NATO governments are increasingly cooperating and jointly investing in cyber security (Shoorbajee, 2018; CCDCOE, 2018). However, their activity is focussed on sharing capabilities (Freedberg, 2018; Emmott, 2018); active measures (Tucker, 2019); cyber norms; international law (Schmitt, 2017); and military approaches (Efthymiopoulos, 2019), but not overall vulnerability reduction. For that, the 'defence in breadth' approach, which is defensive in nature, is the best means to confront vulnerabilities stemming from complexity in cyberspace and to build cyber resilience globally.

Dealing with networked complexity will require more cooperation with manufacturers, which is underway (NATO CCDCOE, 2020), service providers, anti-abuse actors and groups and also technical standards setting bodies and academic researchers. Incorporating these diverse groups is difficult, and not only due to the number of parties. Likely, this will necessitate the development of new tools and approaches to ensure that such cooperation is balanced, technically grounded and sufficiently removed from daily politics. Experts, be they academics, independent, employed by government or private enterprise—must be remunerated and supported when engaging in standard design at bodies like the IEEE and IETF. Security research must be funded and legal frameworks developed to protect bona fide independent researchers from legal repercussions, including by private actors trying to silence inconvenient facts and findings (Lee, 2020; disclose.io, 2020). Only by leveraging this combined expertise will it be possible for states to keep up with developments in computing and cyber security.

NATO and Western governments should also increase their activities against key enablers in cyberspace. These include payment processors that work

with criminals (Levchenko et al., 2011), domain registrars that allow attackers to register domain names and 'bulletproof' hosts that specialise in keeping online malicious sites. Such critical nodes can be identified and regulated by state actors through their enforcement capabilities.

Some companies and manufacturers care about their system and data security; others fail to demonstrate due care and diligence. Due to the network effects of globalisation, an individual organisation's vulnerability can harm many others. Therefore, governments must legally enforce better security practices across the board, which does not entail simply banning foreign companies. Instead, states should require baseline security testing, features and management. States must empower experts, rather than the political apparatus, to create standards, requirements and rules. While political oversight is useful, states should primarily fill the role of the enforcer. The cyber security space is complex and solutions require considerable expertise, often garnered through many years of hands-on experience or research.

While legally forcing security baseline requirements on all devices will complicate some intelligence and law enforcement activity, the risk of catastrophic attacks on critical infrastructure and institutions is too great to not pursue this avenue. Unless states and organisations tighten security in breadth, adversaries will find spaces to stage attacks, gather intelligence, host facilitating tools and worse. However, with security in breadth, potential attackers' costs go up, reducing the number of successful attacks.

5. CONCLUSION

This paper discussed the nature of networked complexity and how it affects security both inside and outside cyberspace. As everything is connected, hardening only those systems deemed critical is insufficient for three reasons. First, current heuristics often miss key attack paths because they fail to recognise important relationships. Second, information security entails computer systems and organisations and their functions—an established but nevertheless often ignored fact. By focusing on complex interdependencies, aspects previously deemed uncritical come to the fore: consumer devices, consumer networking equipment and, crucially, social processes. Third, due to the use of contemporary trends like cloud technologies and increasing specialisation, analysing graphs of interlinked systems and resulting risks is especially pertinent.

It is impossible organisationally or nationally to fully compensate for the security risks associated with complexity. However, by tracing dependencies and relationships, analysing potential attack paths and adapting architectures and security strategies, tactics and operations to a networked environment, organisations and governments can raise the bar when it comes to security. Many of these steps will not be technical in nature but organisational, procedural or architectural. Useful tools are already available in the security and security management spaces that can address the outlined complexity

problems, at least to some extent.

Unfortunately, states likely have to enforce better security for vendors and service providers to protect national assets and critical systems. Without state pressure, it is improbable that sufficient numbers of key actors will sufficiently address security. While it may be slightly detrimental to intelligence and law enforcement activities, the best defence for organic societies like those in NATO states remains security in breadth, in addition to hardening key systems. This means establishing a high level of security throughout, from state intelligence systems through to consumer devices. This approach would obstruct future adversarial operations that try to leverage weaknesses in peripheral or non-hardened systems to attack core or critical systems or infrastructure.

6. REFERENCES

Castells, M. (1996) *The Information Age: Economy, Society and Culture*. Cambridge, MA, Blackwell.

Castells, M. (2000) Materials for an exploratory theory of the network society. *British Journal of Sociology*. 51 (1), 5–24.

Castells, M. (2001) Identity and Change in the Network Society. *Interview with Harry Kreisler*. Available from: http://globetrotter.berkeley.edu/people/Castells/castells-con4.html. [Accessed 4th September 2020].

Clarke, P., O'Connor, R. V. & Leavy, B. (2016) A complexity theory viewpoint on the software development process and situational context. In: Perry D.E. and Raffo, R. (eds.) *ICSSP '16: Proceedings of the International Conference on Software and Systems Process. Proceedings of the International Conference on Software and Systems Process 14-15 May 2016, Austin, Texas.* Association for Computing Machinery. pp. 86–90. Available from doi: 10.1145/2904354.2904369.

Collins, R. (1998) The Pentium F00F Bug. *Dr. Dobbs*. 1st May 1998. Available from: https://www.drdobbs.com/embedded-systems/the-pentium-f00f-bug/184410555. [Accessed 15th June 2020].

Connolly, L.Y. & Wall, D.S. (2019) The rise of crypto-ransomware in a changing cyber crime landscape: Taxonomising countermeasures. *Computers & Security.* 87 (101568). Available from: http://www.sciencedirect.com/science/article/pii/S0167404819301336.

Cyber Risk International (2020) *Cyber Threats to the Agriculture Sector.* 7th April 2020. Available from: https://cyber riskinternational.com/2020/04/07/cyber threats-to-the-agriculture-sector/. [Accessed 17th May 2020].

Dally, W. J., Turakhia, Y & Han, S. (2020) Domain-Specific Hardware Accelerators. *Communications of the ACM.* 63 (7), 48-57. Available from: https://cacm.acm.org/magazines/2020/7/245701-domain-specific-hardware-accelerators/fulltext.

defense.gov (2020) *DOD Reaffirms Original JEDI Cloud Award to Microsoft*. 4th September 2020. Available from: https://www.defense.gov/Newsroom/Releases/Release/Article/2337557/dod-reaffirms-original-jedi-cloud-award-to-microsoft/. [Accessed 1st September 2020].

disclose.io (2020) *Response to Voatz's Supreme Court Amicus Brief*. 14th September

2020. Available from: https://disclose.io/voatz-response-letter/. [Accessed 16th September 2020].

Durkheim, E. (1984) *The Division of Labour in Society*. New edition. Basingstoke, Palgrave Macmillan.

Durumeric, Z., Li, F., Kasten, J., Amann, J., Beekman, J. G., Payer, M., Weaver, N. C., Adrian, D., Paxson, V., Bailey, M. D. & Halderman, J. A. (2014) The matter of heartbleed. In: Williamson, C., Akella, A. and Taft, N. (eds.) *IMC 2014: Proceedings of the 2014 Internet Measurement Conference, 5-7 November 2014, Vancouver, Canada.* Association for Computing Machinery. pp. 475-488.

Eddy, M. (2019) Want to Hack a Satellite? It Might Be Easier Than You Think. *PC Mag*. 7th March 2019. Available from: https://uk.pcmag.com/news/119996/want-to-hack-a-satellite-it-might-be-easier-than-you-think. [Accessed 5th December 2019].

Efthymiopoulos, M. (2019) A cyber security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*. 8 (12). Available from: doi:10.1186/s13731-019-0105-z.

Emmott, R. (2018) NATO cyber command to be fully operational in 2023. *Reuters*. 16th October 2018. Available from: https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9. [Accessed 15th September 2020].

Evans, D. (2011) The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. *CISCO White Paper*. April 2011. Available form: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. [Accessed 5th March 2019].

Fathi, B. (2018) What Really Happened with Vista: An Insider's Retrospective. *Medium*. 3rd January 2018. Available from: https://medium.com/@benbob/what-really-happened-with-vista-an-insiders-retrospective-f713ee77c239. [Accessed 3rd May 2020].

Freedberg, S. (2018) NATO To 'Integrate' Offensive Cyber by Members. *Breaking Defense*. 16th November 2018. Available from: https://breakingdefense.com/2018/11/nato-will-integrate-offensive-cyber by-member-states/. [Accessed 14th September 2020].

Gillis, T. (2016) Complexity is the enemy of security. *Network World*. 8th August 2016. Available from: https://www.networkworld.com/article/3103474/complexity-is-the-enemy-of-security.html. [Accessed 5th November 2017].

Goldstein, J. (2011) Emergence in Complex Systems. In: Allen, P., Maguire, S. & McKelvey, B. (eds.) *The SAGE Handbook of Complexity and Management*. London, Sage. pp. 65-78.

Google Project Zero (2020) *About Project Zero*. Available from: https://googleprojectzero.blogspot.com/p/about-project-zero.html. [Accessed 4th July 2020].

Gilli, A. & Gilli, M. (2019) Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security*. 43(2), 141-189.

Greenberg, A. (2014) Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers. *Wired*. 15th July 2014. Available from: https://www.wired.com/2014/07/google-project-zero/. [Accessed 29th April 2018].

Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. (2013) Internet of Things (IoT): A vision, architectural elements and future directions. *Future Generation Computer Systems*. 29 (7), 1645–1660. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0167739X13000241?via%3Dihub.

Hansen, I. & Lim, D.J. (2019) Doxing democracy: influencing elections via cyber voter interference. *Contemporary Politics*. 25 (2), 150-171.

Hirsch, P., Fiss, P. C. & Hoel-Green, A. (2009) A Durkheimian approach to globalisation. In: Adler, P. (eds.) *The Oxford Handbook of Sociology and Organisation Studies*. Oxford, Oxford University Press. pp. 223-245.

Herkert, J., Borenstein, J. & Miller, K. (2020) The Boeing 737 MAX: Lessons for Engineering Ethics. *Science and Engineering Ethics*. Available from: doi:10.1007/s11948-020-00252-y.

Hutter, B. (2001) *Regulation and Risk: Occupational Health and Safety on the Railways.* Oxford, Oxford University Press.

International Standards Organisation (2018) *ISO/IEC 27000:2018 Information technology. Security techniques. Information security management systems. Overview and vocabulary.* Available from: https://www.iso.org/standard/73906.html. [Accessed 25th November 2020].

Jeangène Vilmer, J.B. (2018) Successfully Countering Russian Electoral Interference. *CSIS Briefs*. June 2018. Available from: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180621_Vilmer_Countering_russiam_electoral_influence.pdf [Accessed 5th July 2020].

Kernighan, B.W. & Pike, R. (1984) *The Unix Programming Environment.* Upper Saddle River, Prentice Hall.

Kliem, R. (2004) Managing the Risks of Offshore in Development Projects. *EDPACS.* 32 (4), 12-20. Available from: Doi:10.1201/1079/44633.32.4.20041001/83712.2.

Krugman, P. (1980) Scale Economies, Product Differentiation and the Pattern of Trade. *The American Economic Review*, 70 (5), 950-959. Available from http://www.jstor.org/stable/1805774.

Krugman, P (1981) Intraindustry Specialisation and the Gains from Trade. *Journal of Political Economy*. 89 (5), 959–973. Available from: https://www.journals.uchicago.edu/doi/10.1086/261015.

Lee, T. (2020) Online voting vendor Voatz urges Supreme Court to limit security research. *Ars Technica*. 8th September 2020. Available from: https://arstechnica.com/tech-policy/2020/09/online-voting-vendor-voatz-urges-supreme-court-to-limit-security-research/. [Accessed 12th September 2020].

Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Felegyhazi, M., Grier, C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H., McCoy, D., Weaver, N., Paxson, V., Voelker, G. M. & Savage, S. (2011) Click Trajectories: End-to-End Analysis of the Spam Value Chain. *Proceedings of the IEEE Symposium on Security and Privacy, 22-25 May 2011, Oakland, California.* Institute of Electrical and Electronics Engineers. pp. 431-446.

Mahutga, M. C. (2012) When do value chains go global? A theory of the spatialisation of global value chains. *Global Networks*, 12 (1), 1-21.

MariaDB Foundation (2020) *About*. Available from: https://mariadb.org/about/. [Accessed 14th August 2020].

Mathews, L. (2017) NotPetya ransomware attack cost shipping giant Maersk over $200 million. *Forbes Magazine*. 16th August 2017. Available from: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/ [Accessed 3rd February 2018].

Meltdownattack.com (2020) *About.* Available from: https://meltdownattack.com/.

[Accessed 5th May 2020].

Meola, A. (2020) Smart Farming in 2020: How IoT sensors are creating a more efficient precision agriculture industry. *Business Insider*. Available from: https://www.businessinsider.com/smart-farming-iot-agriculture. [Accessed 28th November 2020].

Nakashima, E. (2016) Russian government hackers penetrated DNC, stole opposition research on Trump. *The Washington Post*. 16th June 2016. Available from: https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html [Accessed 28th November 2020].

National Institute of Food and Agriculture (2020) *Agriculture Technology*. Available from: https://nifa.usda.gov/topic/agriculture-technology [Accessed 3rd September 2020].

National Information Technology Laboratory (2020) *NIST 800-53. Revision 5. Security and Privacy Controls for Information Systems and Organizations.* September 2020. Available from: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

NATO CCDCOE. (2018) *Japan to Join the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn*. Available from: https://www.ccdcoe.org/news/2018/japan-to-join-the-nato-cooperative-cyber defence-centre-of-excellence-in-tallinn/. [Accessed 12th September 2020].

NATO CCDCOE (2020) *Siemens and NATO CCDCOE advance cooperation on cyber security for critical infrastructure*. Available from: https://ccdcoe.org/news/2020/siemens-and-nato-ccdcoe-advance-cooperation-on-cyber security-for-critical-infrastructure/. [Accessed 20th September 2020].

Nelson, P. (2016) Major cloud is infested with malware, researchers say. *Network World*. 10th November 2016. Available from: https://www.networkworld.com/article/3137260/major-cloud-is-infested-with-malware-researchers-say.html. [Accessed 28th March 2018].

Nielsen, R.A. (2016) Case Selection via Matching. *Sociological Methods & Research*. 45 (3), 569-597. Available from: https://www.mit.edu/~rnielsen/Case%20Selection%20via%20Matching.pdf.

Price, D. (1995) Pentium FDIV flaw-lessons learned. *IEEE Micro*.15 (2), 86-88. Available from: https://ieeexplore.ieee.org/abstract/document/372360.

Popper, K. (2013) *The Open Society and Its Enemies*. Princeton, Princeton University Press.

Purser, S. (2004) Improving the ROI of the security management process. *Computers & Security*. 23 (7), 542-546. Available from: http://www.sciencedirect.com/science/article/pii/S0167404804002329.

Schelling, T. (2006) *Micro Motives and Macro Behavior*. 1st edition. New York, Norton.

Schmitt, N. (ed) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge, Cambridge University Press.

Schneier, B. (2002) The Case for Outsourcing Security. *Computer.org.* April 2002. Available from: https://www.computer.org/csdl/magazine/co/2002/04/r4s20/13rRUxNmPJg. [Accessed 24th July 2018].

Schneier, B. (2003) *Beyond Fear: Thinking Sensibly about Security in an Uncertain World.* Göttingen, Copernicus Books.

Schostack, A. (2014) *Threat Modeling: Designing for Security*. New York, Wiley.

Schostack, A. (2018) *Threat Modeling: What, Why and How?* MISTI Institute. 3rd July 2018. Available from: https://misti.com/infosec-insider/threat-modeling-what-why-and-how. [Accessed 20th January 2020].

Shimpi, A.L. (2012) The iPhone 5's A6 SoC: Not A15 or A9, a Custom Apple Core Instead. *AnandTech*. 15th September 2012. Available from: https://www.anandtech.com/show/6292/iphone-5-a6-not-a15-custom-core. [Accessed 14th September 2020].

Shoorbajee, Z. (2018) Australia and Portugal join NATO cyber cooperative. *Cyber scoop*. 23th April 2018. Available from: https://www.cyber scoop.com/australia-portugal-nato-ccdcoe/. [Accessed 16th September 2020].

Singh, J., Pasquier, T., Bacon, J., Ko, H. & Eyers, D. (2015) Twenty Cloud Security Considerations for Supporting the Internet of Things. *IEEE Internet of Things Journal*. 3 (3), 269 - 284. Available from: doi:10.1109%2FJIOT.2015.2460333.

Taub, A. (2016) D.N.C. Hack Raises a Frightening Question: What's Next? *The New York Times*. 29th July 2016. Available from: http://static.cs.brown.edu/people/jsavage/VotingProject/2016_07_29_NYT_What'sNextAfterDNCHack.pdf. [Accessed 17 September 2020].

Tucker, P. (2019) NATO Getting More Aggressive on Offensive Cyber. *Defense One*. 24th May 2016. Available from: https://www.defenseone.com/technology/2019/05/nato-getting-more-aggressive-offensive-cyber /157270/. [Accessed 8th October 2019].

Vaughan, D. (1996) *The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA*. Chicago, University of Chicago Press.

Vaughan, D. (2005) Organisational rituals of risk and error. In: Hutter, B. and Power, M. (eds.) *Organisational Encounters with Risk*. Cambridge, Cambridge University Press. pp. 33-66.

Vijayan, J. (2013) Attackers turning to legit cloud services firms to plant malware. *Computer World*. 2nd August 2013. Available from: https://www.computerworld.com/article/2484596/attackers-turning-to-legit-cloud-services-firms-to-plant-malware.html. [Accessed 5th February 2020].

Walsh, J. (2014) *Free Can Make You Bleed*. Available from: http://security.grc-daily.com/dsp_getFeaturesDetails.cfm?CID=3482. [Accessed 20th September 2017].

Weissinger, L. B. (2017) Modelling Trust and Trust-Building Among IT-Security Professionals. *Lecture Notes in Computer Science*. 10292, 557–566. Available from: doi:10. 1007/978-3-319-58460-7_39.

Weissinger, L. B. (2018) *Assessment, Trust, and Cooperation in IT-Security*. PhD thesis. University of Oxford.

Wheeler, E. (2011) *Security Risk Management*. Amsterdam, Elsevier Science.

Wilson, D., Roman, E. & Beierly, I. (2018) PCI DSS and card brands: Standards, compliance and enforcement. *Cyber Security: A Peer-Reviewed Journal*. 2 (1), 73-82. Available from: https://www.ingentaconnect.com/content/hsp/jcs/2018/00000002/00000001/art00009.

BIOGRAPHIES

Editors

Amy Ertan is a cybersecurity researcher and PhD candidate at Royal Holloway, University of London. She is a predoctoral Cybersecurity Fellow at the Belfer Center at Harvard University's Kennedy School of Government and Visiting Scholar at the NATO CCDCOE where she is researching the security implications of artificial intelligence in warfare. Ertan has spoken frequently on topics relating to cyber security and national defence, including at AFCEA UK, Cranfield University, FS-ISAC EMEA Hubs and at the Hague Conference for Cyber Norms. She is a 2019-2020 Data Protection Fellow with the Institute for Technology and Society (Rio), FS-ISAC Cybersecurity Scholarship recipient (2019), and Cybersecurity Student of the Year (2018, SC Magazine). Ertan holds a BA (Hons) in Philosophy, Politics and Economics from St Hugh's College, University of Oxford. She holds CRTIA and CISSP qualifications.

Kathryn H. Floyd is the Director of William & Mary's Whole of Government Center of Excellence (COE). She is also the director of the e-internship program at the Global Research Institute. Dr. Floyd has taught courses in the Government Department on security and terrorism while conducting research on youth and adolescent developments prior to radicalization. Recently, Dr. Floyd served as the Mass Violence & Terrorism Visiting Fellow at the US Department of Justice. She has been deeply involved with the new national standard, NFPA 3000 (PS): *Active Shooter Hostile Event Response (ASHER) Program*. Dr. Floyd received her PhD in Strategic Studies from S. Rajaratnam School of International Studies, Nanyang Technological University (Singapore). She holds an MA in War Studies from King's College London and a BA in Government from William & Mary.

Piret Pernik is a Researcher of the Strategy Branch of the NATO CCDCOE. Her main research areas are cyber security strategies and policies, horizon scanning and analysis of cyber threats, and the development of military cyber organizations. Prior joining the NATO CCDCOE, she worked as a Research Fellow at the International Centre for Security and Defence (2013-2018), and served as an advisor to the National Defence Committee of the Estonian Parliament, as well as an advisor with the Ministry of Defence. She has written extensively on cyber security, and contributed to academic journals and book chapters. She holds an MA in Social Theory from the Estonian Institute of Humanities, and an MA in International Relations and European Studies from the Central European University.

Tim Stevens is Senior Lecturer in the Department of War Studies, King's College London (KCL), and leads the KCL Cyber Security Research Group. His research focuses on the intersection of technology, politics and global security, particularly the roles of information technologies in shaping and enabling global security practices. He has written extensively on the politics

and governance of cybersecurity, especially in its strategic and international dimensions. Dr. Stevens has a BA (Hons) from University College London and an MA, MRes and PhD in War Studies from King's College London. He is an elected Fellow of the Royal Geographical Society, a Fellow of the Higher Education Academy, and Senior Fellow and Associate Researcher at the Conservatoire national des arts et métiers (Cnam), Paris.

Authors

Chon Abraham is an Associate Professor in the Mason School of Business at William & Mary in Williamsburg, Virginia where her research and teaching involve cyber security-related topics, business intelligence, data management, and health information management. She is a graduate of the US Military Academy at West Point and has a PhD in Management Information Systems from the University of Georgia. Prof. Chon is a Lieutenant Colonel and Cyber Officer in the United States Air Force Reserve based at the Pentagon in the Chief Data Office. She is a Fulbright Scholar to Japan and an Abe Fellow researching cybersecurity strategy at the national level for the US, Japan, and the UK. Prof. Chon publishes in top tier scholarly journals such as MIT Sloan Management Review and co-authored a 2018 book titled *Hacking Healthcare: Understanding Real World Threats*.

Jacopo Bellasio is a Senior Analyst at RAND Europe. Since joining RAND, he has led and contributed to several research projects for public sector clients including the European Commission, the European Defence Agency, the European Parliament, the UK Foreign and Commonwealth Office, and the Dutch Ministry of Defence. Bellasio's research spans the defence and security domain, with recent work covering future trends in cybercrime, the impact of new and emerging technologies on the future battlefield, and conflict analysis and risk assessment in relation to the responsible sourcing of minerals. Prior to joining RAND, he worked with a human rights NGO in Lebanon and at the University of St Andrews. Bellasio holds an MLitt in Middle East and Central Asian Security Studies from the University of St Andrews.

James Black is a Research Leader in the Defence, Security and Infrastructure research programme at RAND Europe, the European arm of the RAND Corporation. Black leads studies for governmental sponsors across NATO, with a focus on defence strategy and policy, on the military and industrial impact of new technologies and other changes in the future operating environment, and on European defence and security. He also designs and delivers strategic-level wargames, including for the UK's Royal College of Defence Studies. Prior to joining RAND, Black worked in UK Parliament. He holds a dual MA-MSc in International Security from Sciences Po Paris and the London School of Economics, along with a BA (Hons) in History from the University of Cambridge.

Joe Burton is a Senior Lecturer in International Security at the New Zealand Institute for Security and Crime Science, University of Waikato, New Zealand and a Marie Curie fellow (MSCA-IF) at Université libre de Bruxelles (ULB), where he is working on the two-year European Commission-funded project

Strategic Cultures of Cyber Warfare (CYBERCULT). Dr. Burton is the author of *NATO's Durability in a Post-Cold War World* (SUNY Press, 2018), editor of *Emerging Technologies and International Security: Machines the State and War* (Routledge, 2020), and his work has been published in *Asian Security*, *Defence Studies*, *Political Science* and with a variety of other leading academic publishers. He is the recipient of the US Department of State SUSI Fellowship, the Taiwan Fellowship, and has been a Visiting Researcher at the NATO CCDCOE.

Joe Cheravitch has served as an analyst focused on information and cyber warfare for over a decade. He is currently a doctoral student at the Department of Defence Studies at King's College London researching the history of Russian information warfare. Cheravitch previously worked as a defence analyst at the RAND Corporation, where he studied Russia's approach to cyber operations and digital influence efforts in the context of Moscow's foreign policy and military posture. In 2014, Cheravitch completed graduate studies at Georgetown University's School of Foreign Service. He served as a psychological operations specialist in the US Army from 2008 to 2012, deploying to both Afghanistan and Iraq. His work includes a contribution to NATO CCDCOE's *International Conference on Cyber Conflict* as well as articles published by the Center for Strategic and International Studies, *TechCrunch*, and a forthcoming piece in the *Journal of Slavic Military Studies*.

Michael Daniel currently serves as President and CEO of the non-profit Cyber Threat Alliance (CTA). CTA enables companies in the cybersecurity field to share threat information in both automated and human ways to improve the security of the global digital ecosystem. Prior to CTA, Daniel served as Special Assistant to President Obama and Cybersecurity Coordinator on the National Security Council Staff from 2012 to 2017. In this role, he led the development of national cybersecurity strategy and policy and ensured that the US government effectively worked with the private sector, NGOs, and other nations. From 1995 to 2012, he worked for the Office of Management and Budget, overseeing the US Intelligence Community and other national security programs.

Luiz A. DaSilva is the Executive Director of the Commonwealth Cyber Initiative (CCI) and the Bradley Professor of Cybersecurity at Virginia Tech. Previously, he held the chair of Telecommunications at Trinity College Dublin, where he served as the Director of CONNECT, the Science Foundation Ireland Research Centre for Future Networks and Communications. His research focuses on distributed and adaptive resource management in wireless networks, and in particular radio resource sharing, dynamic spectrum access, and the application of game theory and machine learning to wireless networks. Prof. DaSilva is a former IEEE Communications Society Distinguished Lecturer, an IEEE Fellow and a Fellow of Trinity College Dublin.

Sally Daultrey is a UK-based research professional, trained at King's College London, specialising in the geopolitics of cyberspace, comparative national cyber policy and the role for science and cyber in regional security strategies. Daultrey serves as Chief Intelligence Analyst for Adenium Group Ltd. She is based in London and Central Asia. Since 2003, she has worked

in the US, the UK, Central Asia, Australia, India, Indonesia and Singapore. From 2010 to date she has worked on contract with research teams and individuals at embassies, universities and private companies, advising on geopolitical risk, research strategy and international relations. Her contributions on global security issues have included book chapters, original research and participation at research forums in the UK and Asia, including at Chatham House, RUSI, UK parliamentary committees and a UN Summit

Franz-Stefan Gady is a Research Fellow with the International Institute for Strategic Studies' (IISS) Cyber, Space and Future Conflict Division. Formerly a Senior Editor at *The Diplomat*, Gady has advised the US and European militaries on structural reform and the future of armed conflict. Prior to joining the IISS, he held various positions at the EastWest Institute, the Project on National Security Reform and the National Defense University. Gady conducted field research in Afghanistan and Iraq, where, among other things, he embedded with the Afghan National Army, NATO forces and Kurdish militias. Gady has also reported from a wide range of countries and conflict zones as a journalist. His writings have featured in *Foreign Policy*, *The Financial Times* and *Foreign Affairs*, among other publications.

Andreas Haggman is Head of Cyber Advocacy – Skills, Innovation and Research in the UK Department for Digital, Culture, Media and Sports. Dr. Haggman holds a PhD in Information Security from Royal Holloway, University of London where his thesis research focused on using wargames for cyber security education. He has also published widely on topics including cyber deterrence, offensive cyber, and national strategies. As well as running cyber wargames with many public and private organisations across the world, Dr. Haggman has guest lectured at the German Command and Staff College, the Swedish Defence University and the NATO Centre of Excellence Defence Against Terrorism. He has previously worked in the video games, defence and insurance sectors.

Joshua Kenway is a Cybersecurity Associate at the Cyber Threat Alliance and a Research Fellow with the Algorithmic Justice League. He holds an MA in International Policy from Stanford University, where he focused on cybersecurity and digital policy issues. His professional and academic work straddles the intersection of technology, ethics, and security.

Juha Kukkola (Captain, Finnish Defence Forces) has served in the Finnish Defence Forces (FDF) since 2008 as a platoon leader, signals officer, staff officer and lecturer. Dr. Kukkola is specialised in air defence, C4 systems, and Russian and Cyber studies. He is currently attending the General Staff Officer Course at the Finnish National Defense University. His doctoral dissertation, *Digital Soviet Union* examines how the Russian Federation is constructing its national segment of internet based on Soviet-era ideas. Dr. Kukkola is the co-author of *Game Changer and Game Player*, the FDF Research Agency's publications that analyse the strategic implications of Russia's internet policy.

Martin C. Libicki holds the Keyser Chair of Cybersecurity Studies at the

US Naval Academy. In addition to teaching, he carries out research in cyberwar and the general impact of information technology on domestic and national security. Prof. Libicki is the author of a 2016 textbook on cyberwar, *Cyberspace in Peace and War*, as well as *Conquest in Cyberspace: National Security and Information Warfare* and various related RAND monographs such as *Cyberwar and Cyberdeterrence*. Prior employment includes twelve years at the National Defense University, three years on the Navy Staff (logistics) and three years for the US Government Accountability Office. Prof. Libicki holds a PhD from the University of California, Berkeley.

Bilyana Lilly leads project teams and co-authors reports at the RAND Corporation on Russian cyber threat actors, information warfare, election cybersecurity, disinformation, machine learning for text analysis and NATO. She has presented research at professional conferences, including NATO CCDCOE's *International Conference on Cyber Conflict*, *DefCon*, and the Warsaw Security Forum. She received a Key Contributor Medal Award for her work on RAND's election cybersecurity project, which received a Medal Honoring Excellence from RAND's Office of the President. Prior to joining Pardee RAND, Lilly was an associate at the Brookings Institution and also worked at the United Nations Conference on Disarmament in Geneva, Switzerland. She is the author of the book *Russian Foreign Policy Toward Missile Defense*. Lilly has an MA (*summa cum laude*) in Russian and East European studies from the University of Oxford, and an MA in International Affairs from the Graduate Institute in Geneva, Switzerland.

Alice Lynch was previously a Defence and Security Analyst at RAND Europe, where her research focused on national security, strategic decision-making and capability development and European defence and security, with a particular focus on emerging technologies and their defence and security implications. She is now a Specialist at the UK's House of Commons Foreign Affairs Select Committee, where she provides policy support and manages inquiries scrutinising the work of the Foreign, Commonwealth and Development Office. Lynch holds an MA in Applied Security Strategy from the University of Exeter.

Jerry Park is a Professor in the Department of Electrical and Computer Engineering at Virginia Tech and is the Site Director of an NSF Industry-University Cooperative Research Center called Broadband Wireless Access & Applications Center (BWAC). Prof. Park served as an Executive Committee member of the US National Spectrum Consortium (NSC) from 2016 to 2018. His research interests include dynamic spectrum sharing, emerging wireless technologies, wireless security and privacy, and applied cryptography. He is a recipient of a 2017 Virginia Tech College of Engineering Dean's Award for Research Excellence, a 2015 Cisco Faculty Research Award, a 2014 Virginia Tech College of Engineering Faculty Fellow Award, and a 2008 NSF CAREER Award. Prof. Park is currently serving as the Steering Committee Chair of the IEEE Symposium on Dynamic Spectrum Access Networks (DySPAN). He is an IEEE Fellow for

his contributions to dynamic spectrum sharing and related security issues. **Jeffrey H. Reed** is the founder of Wireless@Virginia Tech, and served as its director until 2014. He is the founding faculty member of the Ted and Karyn Hume Center for National Security and Technology and served as its interim director when founded in 2010. In 2005, Prof. Reed became Fellow to the IEEE for contributions to software radio and communications signal processing and for leadership in engineering education. In 2013 he was awarded the International Achievement Award by the Wireless Innovations Forum. In 2012 he served on the President's Council of Advisors of Science and Technology advisory group that examined ways to transition federal spectrums for commercial use. Prof. Reed is a past member of CSMAC, a group that provides advice to the National Telecommunications and Information Administration (NTIA) on spectrum issues.

Erik Silfversten is the Co-Director of the RAND Europe Centre for Future and Foresight Studies (CFFS) where he works at the intersection of technology, policy, and the future. His primary research interests are complex, strategic policy challenges in relation to cybersecurity and emerging technologies. Silfversten has extensive experience in policy research for governments and international organisations, including the European Union Agency for Cybersecurity (ENISA), European Commission, European Defence Agency, NATO, and various ministries of defence. Prior to joining RAND, he held the position of manager for policy and strategic development at IMPACT, the cyber security partner of the International Telecommunication Union (ITU). Erik holds an MSc (Hons) in International Relations and Global Issues from the University of Nottingham.

Sachin Shetty is an Associate Director in the Virginia Modeling, Analysis, and Simulation Centre and holds a joint appointment as an Associate Professor with the Department of Computational Modeling and Simulation Engineering at Old Dominion University. His research interests lie at the intersection of computer networking, network security, and machine learning. Prof. Shetty has authored over 140 research articles in journals and conference proceedings and edited four books. He serves as the chair for the IEEE P2418.6 Internet of Medical Things Standards group. Prof. Shetty is the recipient of Fulbright Specialist award, EPRI Cybersecurity Research Challenge award, DHS Scientific Leadership Award and has been inducted in Tennessee State University's Million Dollar Club. He is a Senior Member of IEEE and a Commonwealth Cyber Initiative Fellow.

Simona R. Soare is a Senior Associate Analyst at the European Union Institute of Security Studies (EUISS). Her research focuses on transatlantic and European security and defence, EU-NATO cooperation and defence innovation. Prior to joining EUISS, Soare served as an advisor to the Vice-President of the European Parliament (2015-2019) and as an analyst with the Romanian Ministry of Defence. She lectured in international relations in Romania, Belgium and France and she is a regular contributor to CSDP courses with the European Security and Defence College. Soare holds a PhD in Political Science and she is a US Department of State fellow. She

has published extensively on American and European security and defence, including defence capability development, emerging technologies and defence innovation, arms transfers, export controls and regional defence.

Alexander Stronell is a Research Assistant with the International Institute for Strategic Studies' (IISS) Cyber, Space and Future Conflict Division. Alexander joined the IISS after completing a dual master's degree in International Relations and Security from Sciences Po, Paris and Moscow State Institute of International Relations (MGIMO). A recipient of a Leverhulme Trust scholarship, his Master's research addressed the relationship between Russian domestic politics and the Kremlin's foreign policy choices. Prior to his graduate studies, Alexander obtained a First Class BA (Hons) in History from the University of Oxford. He joined the IISS following a work placement with the Atlantic Council's Transatlantic Security Initiative in Washington DC.

Olesya Tkacheva is Assistant Professor at Vesalius College and Free University of Brussels (VUB). Her research focuses on the nexus between technology and security. During 2018-2019 she was Acting Dean of Vesalius College. Prior to moving to Brussels, she worked for the RAND Corporation and the US Department of Defense and was a Post-Doctoral Fellow at the University of Rochester. She is a winner of the National Science Foundation Graduate Fellowship and Fulbright Fellowship to Russia. She holds a PhD from the University of Michigan.

Haining Wang is a Professor of Electrical and Computer Engineering at Virginia Tech. His research interests lie in the areas of security, networking system, and cloud computing. He is currently an Associate Editor for IEEE *Transactions on Cloud Computing* and *Journal of Computer Security*. He was the TPC Co-Chair for the 50th IEEE/IFP *International Conference on Dependable Systems and Networks*. He is a Fellow of the IEEE. Prof. Wang received his PhD degree in computer science and engineering from the University of Michigan.

Laurin B. Weissinger is a Lecturer at the Fletcher School and a researcher with the Computer Science Department, Tufts University. He is also the Visiting Cybersecurity Fellow at Yale Law School, and a Visiting Fellow at the Information Society Project at Yale Law School. He is currently serving as a Vice Chair of the Second Security, Stability, and Resiliency Review (SSR2) for the International Corporation of Assigned Names and Numbers (ICANN). His research focuses on international and organisational cyber security, with a focus on risk, complexity, privacy, infrastructure, and regulation. Laurin holds a DPhil and MSc from the University of Oxford and an MPhil from the University of Cambridge. He is a Certified Information Systems Security Professional (CISSP).

Cindy Whang is an Assistant Professor at Fu Jen Catholic University in Taiwan and the Interim Director for the School of Continuing Education Law Department. She received her SJD from the University of Wisconsin Law School and had worked extensively in coordinating US-foreign government training programs and international academic cooperation

for the University of Wisconsin Law School East Asian Legal Studies Center. Her papers have been published in the *Journal of International Economic Law*, *Wisconsin International Law Journal*, and other international publications.

Duminda Wijesekera is the Acting Chair of the newly formed Cyber Security Engineering Department and a Professor in the Department of Computer Science at George Mason University, Fairfax, Virginia and a visiting research scientist at the National Institute of Standards and Technology (NIST). He leads the Laboratory of Radio and RADAR Engineering.