UNIVERSITY OF EXETER | STRATEGY AND SECURITY INSTITUTE

Should NATO Adopt a Joint Offensive Cyber Capability?

University of Exeter

This dissertation is submitted for the degree of Master of Arts in Applied Security Strategy

Word Count: 10,968

September 2020

Abstract

Over the past decade, there has been a steep increase in cyberattacks targeting NATO members' military and critical infrastructure. The Transatlantic Alliance faces hundreds of significant hacking attempts every month, launched by state and non-state actors. The measures NATO has taken in response have almost all been defensive in nature, such as committing to advancing defence cooperation in its 2010 Strategic Concept. However, NATO has already begun to reverse this defensive posture by establishing the Mons Cyberspace Operations Centre in 2018, which hopes to integrate individual members' offensive cyber capabilities to deter and defend against threats. Crucially, though, NATO commanders have no operational authority over the use of these weapons, while the Alliance has declared that it has no plans to develop joint offensive cyber capabilities. This dissertation argues this presents various problems for NATO's raison d'être: deterring aggression and collective defence. It argues that pooling members' sovereign offensive cyber capabilities under a joint command and control structure would likely improve cyber-deterrence and would certainly improve collective defence. Adopting a cyber deterrence-by-punishment posture would bolster and complement NATO's current cyber deterrence-by-denial approach. Despite these likely benefits, however, NATO would need to overcome several practical and legal problems to establish a joint offensive cyber capability. Accordingly, this thesis's main argument and recommendation is as follows: NATO *should* acquire a joint offensive cyber capability *in the future* for the purpose of cyber-deterrence and collective defence, even though practical and legal obstacles would make this unrealistic to achieve in the short-term.

Table of Contents

List of Abbreviations

A2/AD	Anti-Access/ Area Denial
C2	Command and Control
CCD CoE	Cooperative Cyber Defence Centre of Excellence
CIA	Central Intelligence Agency
CPG	Cyber Planning Group
CyOC	Cyberspace Operations Centre
DDoS	Distributed Denial of Service
EFP	Enhanced Forward Presence
EU	European Union
EW	Electronic Warfare
FDO	Flexible Deterrent Options
GDP	Gross Domestic Product
GPS	Global Positioning System
IHL	International Humanitarian Law
IT	Information Technology
JISD	Joint Intelligence and Security Division
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organisation
NPG	Nuclear Planning Group
NSA	National Security Agency
SACEUR	Supreme Allied Commander Europe
SCADA	Supervisory Control and Data Acquisition
UK	United Kingdom
UN	United Nations
US	United States
USAF	United States Air Force
USCYBERCOM	US Cyber Command

Introduction

Ever since the devastating 2007 cyberattacks that crippled Estonia by shutting down the online services of government ministries, major banks and media outlets, NATO's posture in cyberspace has had to constantly evolve.[1] Over the past decade, there has been a steep increase in cyberattacks targeting NATO members' military and critical infrastructure.[2] The measures NATO has taken in response have almost all been defensive in nature, such as committing to advancing defence cooperation in its 2010 Strategic Concept.[3] However, the Alliance has already begun to reverse this defensive mandate in cyberspace by establishing the Mons Cyberspace Operations Centre (CyOC) in 2018, which hopes to integrate individual members' offensive cyber capabilities into Alliance operations.[4] Crucially, though, NATO commanders have no control over the use of these weapons, while the Alliance has declared that it has no plans to develop joint offensive cyber capabilities.[5] This paper argues this presents

[1] Vincent Joubert, 'Five Years After Estonia's Cyber Attacks: Lessons Learned For NATO?', *NATO Defence College*, 76, (2012), 1; BBC News, 'How a Cyber Attack Transformed Estonia', *BBC News*, (2017), last accessed on (09/09/2020), https://www.bbc.co.uk/news/39655415#:~:text=On%2026%20April%202007%20Tallinn,in%20some%20cases%20lasted%20weeks.&text=Such%20attacks%20are%20not%20specific%20to%20tensions%20between%20the%20West%20and%20Russia.

[2] Ion Iftimie, 'NATO's Needed Offensive Cyber Capabilities', *NATO Defence College Policy Brief*, (2020), last accessed on (09/09/2020), http://www.ndc.nato.int/download/downloads.php?icode=643, 1-2.

[3] Rex Hughes, 'NATO and Cyber Defence: Mission Accomplished?', *Atlantisch Perspectief*, 33, (2009), 1; NATO, 'Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization', *NATO*, (2010), last accessed on (09/09/2020), https://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf, 16.

[4] Reuters, 'NATO Cyber Command to be Fully Operational in 2023', *Reuters*, (2018), last accessed on (09/09/2020), https://uk.reuters.com/article/uk-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUKKCN1MQ1ZT.

[5] Mark Pomerleau, 'Here Are the Problems Offensive Cyber Poses for NATO', *Fifth Domain*, (2019), last accessed on (09/09/2020), https://www.fifthdomain.com/international/2019/11/20/here-are-the-problems-offensive-cyber-poses-for-nato/; NATO, 'NATO Cyber Defence Fact Sheet', *NATO*, last accessed on (09/09/2020), https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf.

various problems for NATO's cyber-deterrence and collective defence, which a joint offensive cyber capability would go a long way to resolve.

This dissertation fills an important gap in the existing literature on this subject. On a national level, NATO allies now publicly acknowledge the importance of cyberweapons – which until recently were a taboo topic to discuss – in an age of hybrid warfare.[6] The UK's Russia report, released in July 2020, says developing offensive cyber capabilities is 'essential' to combat Moscow's cyberattacks.[7] Meanwhile, there is a lively academic debate over the strengths and limitations of deterrence-by-denial and deterrence-by-punishment in cyberspace, which has yielded little consensus. Separately, some academics argue that deterrence-by-punishment is important in strengthening NATO's current deterrence-by-denial posture, some advocating the use of offensive cyber capabilities to achieve this.[8] However, very few have actually argued that NATO should acquire *collective* offensive cyber capabilities over which it has operational authority and oversight.[9]

Definitions

A 'joint offensive cyber capability' is defined as one where allies' sovereign cyber-sabotage capabilities are pooled together under a joint command and control (C2) structure, similar to NATO's conventional command structure. In essence, this would be a more cooperative version of the Mons CyOC, where information is more transparent and NATO commanders have operational authority instead of member

[6] National Public Radio, 'How The U.S. Hacked ISIS', *National Public Radio,* (2019), last accessed on (09/09/2020), https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis?t=1599413589681.
[7] United Kingdom, Intelligence and Security Committee of Parliament, 'Russia Report', (2020), last accessed on (09/09/2020), https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl, 7.
[8] James Lewis, 'The Role of Offensive Cyber Operations in NATO's Collective Defence', *Tallinn Paper,* 9, (2015), 2; Susan Davis, 'NATO In The Cyber Age: Strengthening Security & Defence, Stabilising Deterrence', *NATO Parliamentary Assembly*, (2019), last accessed on (09/09/2020), https://nato-pa.int/download-file?filename=sites/default/files/2019-10/REPORT%20148%20STC%2019%20E%20rev.%201%20fin%20%20-%20NATO%20IN%20THE%20CYBER%20AGE.pdf, 7.
[9] Iftimie, 'NATO's Needed Offensive Cyber Capabilities', 4.

states. 'Cyber-sabotage' is a type of cyberattack that aims to disrupt, deceive, or destroy an adversary's computer systems and networks with the aim of rendering them unavailable, untrustworthy or less useful.[10]

In this dissertation, the *purpose* of such a capability is to strengthen NATO's cyber-deterrence and collective defence against state and non-state actors. This is because NATO's raison d'être centres on deterring aggression and collective defence.[11] State and non-state actors are the chosen referent object, because both conduct cyberattacks against NATO.[12] Furthermore, NATO's main state adversaries in cyberspace, Russia and China, frequently use non-state hacking groups to conduct attacks on their behalf.[13]

Cyber deterrence-by-punishment is defined as deterring cyberattacks by threatening painful retaliation and the imposition of unacceptable costs on an aggressor via cyber-sabotage.[14] Conversely, cyber deterrence-by-denial is the concept of using strong cyber defences to deter an aggressor by convincing them there will be no gains commensurate with the cost of attack.[15]

Structure, Research Questions and Argument

Chapter 1 begins by outlining NATO's history with cybersecurity and its current cyber doctrine. It also explains what cyberweapons are in more detail, before introducing the academic debates over cyber-deterrence. Chapter 2 then explores this debate in more depth, before addressing the first of three research questions, which

[10] Herbert Lin, 'Offensive Cyber Operations and the Use of Force', *Journal of National Security Law & Policy*, 4, (2010), 63.

[11] NATO, 'Deterrence and Defence', *NATO*, (2020), last accessed on (09/09/2020), https://www.nato.int/cps/en/natohq/topics_133127.htm.

[12] Iftimie, 'NATO's Needed Offensive Cyber Capabilities', 2.

[13] Johan Sigholm, 'Non-state Actors in Cyberspace Operations', *Journal of Military Studies*, 4:1, (2013), 16; Reuters, 'NATO Cyber Command to be Fully Operational in 2023'.

[14] Kenneth Geers, 'The Challenge of Cyber Attack Deterrence', *Computer Law & Security Review*, 26:3, (2010), 301.

[15] İhsan Burak Tolga, 'Principles of Cyber Deterrence and the Challenges in Developing a Credible Cyber Deterrence Posture', *NATO CCDCOE*, (2018), last accessed on (09/09/2020), https://pdfs.semanticscholar.org/9549/e0fc5b5e87fad6979d9d910eb10e25dbdeab.pdf, 7.

is: would a joint offensive cyber capability improve NATO's cyber-deterrence and collective defence? It argues that it would likely improve the former and that it would certainly enhance the latter. Chapter 3 answers the second research question: would such a capability be practical to establish? It argues that there are several key obstacles that would need to be overcome, namely: political leaders' reluctance to use cyberweapons; the Alliance's lacking cohesion; and, most importantly, national intelligence agencies' great reluctance to share information necessary for effective cyber-sabotage operations. Chapter 4 addresses the third research question: would such a capability be legal to establish and use? It argues that although it would be legal in certain circumstances, NATO would need to overcome several challenges in three areas: deciding when to retaliate in cyberspace; abiding by international law when launching cyberattacks; and pooling sovereign capabilities in the first place.

Chapter 5 gives recommendations for future course of action based on the previous chapters' arguments. The first recommendation doubles up as the conclusive answer to this dissertation's title question: **NATO *should* acquire a joint offensive cyber capability *in the future* for the purpose of cyber-deterrence and collective defence, even though practical and legal obstacles would make this unrealistic to achieve in the short-term**. This offensive posture should *complement* the current defensive one, not replace it, while a joint cyber capability must be seen as another tool in the arsenal, not a 'silver bullet'. Chapter 5 also recommends the Alliance take several measures now to prepare the ground for this future acquisition.

Chapter 1: Background

This chapter is split into two sections. The first provides a brief overview of NATO's history with cybersecurity and its current cyber doctrine. The second gives some background to what offensive cyber capabilities are and how they can be used. It also introduces the academic debates over cyber-deterrence, a concept that cannot be ignored when discussing an international organisation tasked with deterring aggression.

NATO and Cybersecurity

The devastating 2007 cyberattacks on Estonian information systems and telecommunication networks served as a true wake-up call for NATO.[16] It demonstrated that even an unsophisticated attack could cripple a country dependent on IT networks.[17] Meanwhile, combined cyber and kinetic attacks on Georgia during Russia's 2008 invasion showed similar techniques could be employed in a conventional war.[18] This watershed moment in the evolution of warfare propelled NATO to debate its future in the cyber domain.[19] At the 2008 Bucharest Summit, NATO created the Cyber Defence Management Authority to 'centralise cyber defence operational capabilities across the Alliance'.[20] In the same year it created the Cooperative Cyber Defence Centre of Excellence (CCD CoE), to deal with cyber defence education, consultation and R&D.[21] Following this, NATO adopted a new Strategic Concept in Lisbon 2010, which formally acknowledged the cyber threats the Alliance faces and advanced defence cooperation, by committing to coordinating

[16] Joubert, 'Five Years After Estonia's Cyber Attacks: Lessons Learned For NATO?', 1.

[17] Ibid.

[18] NATO, 'Cyber Defence', *NATO*, (2020), last accessed on (09/09/2020), https://www.nato.int/cps/en/natohq/topics_78170.htm.

[19] Stephen Herzog, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses', *Journal of Strategic Security*, 4:2, (2011), 54.

[20] Hughes, 'NATO and Cyber Defence: Mission Accomplished?', 1.

[21] NATO, 'Cyber Defence'.

'national cyber-defence capabilities' and 'bringing all NATO bodies under centralised cyber protection'.[22] Despite this, it was not clear where the task of countering cyber threats fitted among the Alliance's core commitments.[23] By contrast, the allies adopted an enhanced policy at the 2014 Wales summit, establishing cyber defence as a '*core* task' and prioritising the protection of NATO-owned networks.[24] This extra focus on cyber-threats was epitomised by NATO's 2014 decision that a cyberattack could trigger the Alliance's Article 5 collective defence clause.[25]

However, while triggering Article 5 in response to a cyberattack seemed a distant prospect in 2014, in 2016 it became more of a reality. In 2016, Yahoo acknowledged that at least 500 million of its accounts were hacked in 2014 in what appeared to be the world's largest cyber breach to date.[26] 2016 also saw the first major attack on the Internet of Things, when DYN Corporation servers were disrupted following the hacking of devices like digital cameras.[27] This attack, the biggest of its type ever, brought down much of America's internet for a day.[28] While cyberattacks had once been a concern primarily for individual entities like banks or hospitals, 2016

[22] NATO, 'Strategic Concept', 16.

[23] NATO, 'Preparing for Tomorrow: Cyber Defence and the New Strategic Concept', *NATO*, (2011), last accessed on (09/09/2020), https://www.nato.int/cps/en/natolive/news_77515.htm.

[24] NATO, 'Cyber Defence'.

[25] Steve Ranger, 'NATO Updates Policy: Offers Members Article 5 Protection Against Cyber Attacks', *Atlantic Council*, (2014), last accessed on (09/09/2020), https://www.atlanticcouncil.org/blogs/natosource/nato-updates-policy-offers-members-article-5-protection-against-cyber-attacks/.

[26] Reuters, 'Yahoo Says Hackers Stole Data From 500 Million Accounts in 2014', *Reuters*, (2016), last accessed on (09/09/2020), https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-hackers-stole-data-from-500-million-accounts-in-2014-idUSKCN11S16P#:~:text=Yahoo%20says%20hackers%20stole%20data%20from%20500%20million%20accounts%20in%202014,-Dustin%20Volz&text=(Reuters)%20%2D%20Yahoo%20Inc%20YHOO,known%20cyber%20breach%20by%20far.

[27] The Guardian, 'DDoS Attack That Disrupted Internet Was Largest of its Kind in History, Experts Say', *The Guardian*, (2016), last accessed on (09/09/2020), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[28] Ibid.

saw them become an instrument of hybrid warfare, with the state and society under near permanent attack.[29]

Accordingly, NATO stepped up its cyber defence posture as it had after the 2007 attack. It introduced two new measures at the 2016 Warsaw Summit to do this. First, the Alliance declared its recognition of cyberspace as a fifth operational domain alongside land, sea, air and space.[30] This was a significant shift in focus from NATO merely protecting its own internal networks, to protecting every military activity that it carries out.[31] What this meant is that the Alliance committed itself to cyber defence at all three stages of NATO's engagement. These are: pre-crisis situations, including attempts to penetrate its networks; crisis scenarios, where attackers might disrupt NATO's C2 and reinforcement activities; and hot war situations, where access to allied networks might be compromised.[32] The second measure it introduced at Warsaw was the 2016 Cyber Defence Pledge. This committed the allies to strengthening their cyber defences in accordance with the enhanced policy adopted in Wales, as a matter of priority.[33]

But despite these measures, NATO's members have continued to face increasing cyberattacks since 2016, primarily from state actors. In 2017, Russia launched the huge NotPetya attack against Ukraine, wiping data from the computers of banks, energy firms, senior government officials and an airport.[34] Although Ukraine is not part of the Alliance, the virus still affected member states because it spread to the rest of the world. It crippled the Danish shipping company Maersk and

[29] Jamie Shea, 'NATO: Stepping Up Its Game in Cyber Defence', *Cyber Security: A Peer-Reviewed Journal*, 1:2, (2017), 167.
[30] NATO, 'Cyber Defence'.
[31] Shea, 'NATO: Stepping Up Its Game in Cyber Defence', 167.
[32] Ibid, 167-8.
[33] NATO, 'Cyber Defence Pledge', *NATO*, (2016), last accessed on (09/09/2020), https://www.nato.int/cps/en/natohq/official_texts_133177.htm.
[34] The Washington Post, 'Russian Military was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes', *The Washington Post*, (2018), last accessed on (09/09/2020), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

the American pharmaceutical giant Merck, causing an estimated $10 billion in damages.[35] NATO itself faces hundreds of significant hacking attempts every month, principally from Russia, North Korea and China.[36] Though Russia is NATO's main adversary in cyberspace, China should not be underestimated. Although there is no irrefutable evidence that China has carried out cyber-sabotage attacks, it does focus heavily on cyber-espionage.[37] China is increasingly stealing NATO members' intellectual property via espionage techniques, the most prominent example being its theft of Lockheed Martin's blueprints for the F-35 fighter jet in 2007.[38]

NATO takes cybersecurity seriously for good reason. The highly developed nations that constitute most of its membership depend heavily on cyberspace. Critical infrastructure like pipelines rely on Supervisory Control and Data Acquisition (SCADA) systems that are not designed to be resilient to cyberattacks.[39] NATO and its partners have already suffered crippling SCADA attacks, such as that on the Ukrainian Power grid in 2015 and the 2014 Dragonfly attack on more than 1000 energy companies.[40] Worldwide, the functioning of society and the economy will increasingly depend on cyberspace too. Estimates suggest there will be 125 billion devices connected to the internet by 2030, along with almost all European cars too.[41]

[35] Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, (2018), last accessed on (09/09/2020), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[36] Reuters, 'NATO Cyber Command to be Fully Operational in 2023'.

[37] Lyu Jinghua, 'What Are China's Cyber Capabilities and Intentions?', *Carnegie Endowment for International Peace*, (2019), last accessed on (09/09/2020), https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

[38] The National Interest, 'Hacked: How China Stole U.S. Technology for Its J-20 Stealth Fighter', *The National Interest,* (2019), last accessed on (09/09/2020), https://nationalinterest.org/blog/buzz/hacked-how-china-stole-us-technology-its-j-20-stealth-fighter-66231.

[39] Infosec, 'SCADA & Security of Critical Infrastructures', *Infosec*, (2020), last accessed on (09/09/2020), https://resources.infosecinstitute.com/scada-security-of-critical-infrastructures/#gref; Jeffrey Hunker, 'Cyber War and Cyber Power: Issues for NATO Doctrine', *NATO Defence College*, 62, (2010), 2.

[40] Infosec, 'SCADA & Security of Critical Infrastructures'; BBC News, 'Energy Firms Hacked by 'Cyber-espionage Group Dragonfly', *BBC News*, (2014), last accessed on (09/09/2020), https://www.bbc.co.uk/news/technology-28106478.

[41] Florence Gaub, 'Global Trends to 2030: Challenges and Choices for Europe', *European Strategy and Policy Analysis System,* (2019), last accessed on (09/09/2020),

Meanwhile, NATO's own critical infrastructure is highly vulnerable as well. Its space satellites, which are vital for all operations, are vulnerable to a range of attacks including digital GPS spoofing hacks.[42] Therefore, deterring cyberattacks on everything from mobile phone networks to core military systems is a daunting task of the utmost importance.

Crucially, however, NATO has a defensive mandate in cyberspace, a fact that it reaffirmed in Warsaw.[43] Despite this, it has taken an increasing interest in offensive capabilities. Until recently, NATO member states including the US relied on defensive measures alone to protect their infrastructure. However, this had little deterrent effect, as Chapter 2 explores in more detail. In 2016 and 2018 respectively, key Alliance members Britain and America publicly authorised the use of offensive cyberweapons to deter adversaries.[44] Then, NATO Secretary General Jens Stoltenberg announced in 2017 that the Alliance would integrate members' cyberweapons into military operations to deter and defend against threats.[45] Accordingly, NATO established the CyOC the following year.[46] This departure from NATO's defensive mandate marked the 'biggest overall policy shift in decades', according to officials.[47] Aiming to be fully staffed by 2023, the CyOC's primary mission is to enhance military commanders'

https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/ESPAS_Report2019.pdf, 18.

[42] Beyza Unal, 'Cybersecurity of NATO's Space-based Strategic Assets', *Chatham House*, (2019), last accessed on (09/09/2020), https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf, 5-12.

[43] NATO, 'Cyber Defence'.

[44] United Kingdom, 'National Cyber Security Strategy, 2016 – 2021', (2016), last accessed on (09/09/2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, 51; The Washington Post, 'White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries', *The Washington Post*, (2018), last accessed on (09/09/2020), https://www. washingtonpost.com/world/national-security/trump-authorizes-offensive-cyberoperations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html?utm_term=.1f668d182794.

[45] Sophie Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', *The German Marshall Fund of the United States,* 39, (2018), 4.

[46] Reuters, 'NATO Cyber Command to be Fully Operational in 2023'.

[47] Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', 4.

situational awareness to inform operations and strengthen NATO's cyber defences.[48] Importantly, it also hopes to integrate individual nations' offensive cyber capabilities into Alliance operations, if cyber warfare principles can be agreed.[49] These would be coordinated under the command of the Supreme Allied Commander Europe (SACEUR).[50] According to Reuters, the CyOC could potentially use cyberweapons to destroy enemy missiles, air defences, or computer networks in place of conventional weaponry.[51]

However, what is essential to note for this dissertation is the fact that NATO does not possess its own cyberweapons. Paradoxically, it has declared that, as a defensive Alliance, it will not seek offensive cyber capabilities itself, instead relying on the capabilities of voluntary member states.[52] Under this system, allies fielding sovereign cyberweapons (America, Britain, France and Germany) can volunteer them for Alliance operations, without NATO having any control or oversight over their use.[53] This shift towards offensive cyber seems set to continue. Ion Iftimie, a well-renowned cybersecurity researcher at the NATO Defence College, claims that NATO will look for new ways to integrate cyberweapons into its operations and missions over the next two decades.[54] Overall, NATO is in an interesting if somewhat contradictory position. Despite its mandate of collective defence, it is increasingly leaning towards offensive cyber capabilities to deter and defend. Yet unlike conventional assets, it does not know what capabilities its members possess in cyberspace nor what their effects are. Chapter 2 outlines the problems this poses and the ways in which a NATO-owned capability could overcome these.

[48] NATO, 'NATO Cyber Defence Fact Sheet'.
[49] Reuters, 'NATO Cyber Command to be Fully Operational in 2023'.
[50] Ibid.
[51] Ibid.
[52] Pomerleau, 'Here Are the Problems Offensive Cyber Poses for NATO'; NATO, 'NATO Cyber Defence Fact Sheet'.
[53] Lewis, 'The Role of Offensive Cyber Operations in NATO's Collective Defence', 7; NATO, 'NATO Cyber Defence Fact Sheet'.
[54] Iftimie, 'NATO's Needed Offensive Cyber Capabilities', 1.

Offensive Cyber: What is it?

Cyberweapons are soon to feature in most states' arsenals, with 100 countries actively developing offensive cyber capabilities.[55] As stated in the Introduction, this dissertation defines 'offensive cyber capability' as cyber-sabotage. In practice, this can take several forms and serve different purposes.

There are too many varieties of cyber-sabotage to cover them all, but to give an idea, some of the most common forms include launching a Distributed Denial of Service (DDoS) attack, a virus or a worm. Under DDoS, the attacker attempts to swamp a computer server with requests until it crashes, preventing user access to a network or service.[56] The DDoS attack on DYN Corporation that shut down the internet is a case in point. Viruses can sabotage a computer system from the inside via an infected document, like a Word document.[57] A worm, meanwhile, can self-replicate and destroy a system without a host programme to sustain it.[58] The most famous example is the 2010 Stuxnet attack on Iran's nuclear programme, where an advanced worm spread on its own through the programme's computer network to destroy nuclear centrifuges.[59]

However, the *intentions and effects* of cyberattacks are of greater relevance to this paper than their technical differences. Their most prominent uses for a military organisation like NATO include: disrupting or destroying an enemy's military cyber capability before it can be used; 'hackbacks' to retaliate against the source of a cyberattack; striking strategic targets necessary for warfighting and battlefield close

[55] Max Smeets, 'Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment', *Defence Studies*, 18:4, (2018), 395.
[56] Felix Lau, Stuart Rubin, Michael Smith, and Ljiljana Trajkovic, 'Distributed Denial of Service Attacks', *IEEE*, 3, (2000), 2275.
[57] Kaspersky, 'What is a Computer Virus or a Computer Worm?', *Kaspersky*, (2020), last accessed on (09/09/2020), https://www.kaspersky.co.uk/resource-center/threats/viruses-worms.
[58] Ibid.
[59] David Kushner, 'The Real Story of Stuxnet', *IEEE Spectrum*, 3:50, (2013), 50.

support.[60] The relevance of these effects for cyber-deterrence and defence are discussed in Chapter 2.

There has been little public debate on the purpose of offensive cyber capabilities, while little is known about how states use or expect to use them.[61] This is not surprising, given that until recently they were a taboo topic for governments to discuss.[62] Nonetheless, mapping cyberweapons' capabilities onto Robert Art's four uses of military power – defence, deterrence, compellence and 'swaggering' – helps explain their potential use to states.[63] Generally speaking, cyber-sabotage capabilities are clearly useful for defence and compellence. In terms of defence, they can be used to launch preventative and pre-emptive attacks; Stuxnet, for instance, sought to prevent Iran from gaining a nuclear weapon.[64] Meanwhile, they can compel an adversary to stop an action or do something they would not otherwise do by threatening a cyberattack to enforce compliance.[65] Conversely, states cannot really 'swagger' with such capabilities, because cyber-weapons cannot be publicly displayed and only have a very limited shelf-life before they become obsolete.[66]

Cyber-deterrence, on the other hand, is a far more contested topic. Scholars' positions on cyber-deterrence can be divided into three broad camps. The first group argue cyber deterrence-by-denial and deterrence-by-punishment do work and that

[60] Gregory Rattray and Jason Healey, 'Categorizing and Understanding Offensive Cyber Capabilities and Their Use', in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*, (Washington, DC: National Academies Press, 2010), p. 81.

[61] The Guardian, 'UK To Launch Specialist Cyber Force Able To Target Terror Groups', *The Guardian*, (2020), last accessed on (09/09/2020), https://www.theguardian.com/technology/2020/feb/27/uk-to-launch-specialist-cyber-force-able-to-target-terror-groups; Herbert Lin and Max Smeets, 'Offensive Cyber Capabilities: To What Ends?', *NATO CCDCOE*, (2018), last accessed on (09/09/2020), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8405010&casa_token=4f6mqjiYAIIAAAAA:yHTbI7EpGIGORExYG3SEFEkevH8Y6vLPVpG_gtZUqghqLnLuvJVJerKvHFM8BNn6CbQzik6H&tag=1, 56.

[62] National Public Radio, 'How The U.S. Hacked ISIS'.

[63] Robert Art, 'To What Ends Military Power?', *International Security*, 4:4, (1980), 3-35.

[64] Lin and Smeets, 'Offensive Cyber Capabilities: To What Ends?', 58.

[65] Ibid, 64.

[66] Lin and Smeets, 'Offensive Cyber Capabilities: To What Ends?', 66.

they do not have distinctive problems.[67] Within this group, some argue deterrence-by-punishment is the only viable option because the cyber domain is inherently offense-dominant.[68] Others argue deterrence-by-denial is better, because it is difficult to confidently attribute hacks to a perpetrator and respond in a proportional manner.[69] The second, smaller, group argue cyber-deterrence is very difficult to achieve, but that solutions can be found in certain circumstances. Nye argues that the problems of cyber-deterrence can be overcome by advancing economic interdependence and promoting international norms, depending on the actor one wishes to deter.[70] The final group argue that all forms of cyber-deterrence do not work. Neither deterrence-by-denial nor deterrence-by-punishment are credible, they argue, because the cyber domain is such a complex environment. This complexity has multiple sources: attacks are challenging to attribute; damage assessments are difficult; counterforce is not always possible and signalling one's capabilities is near impossible.[71] Overall, it is important to show how hotly debated cyber-deterrence is, because it goes to the very heart of whether NATO – an organisation that seeks to deter aggression – should adopt a joint offensive cyber capability. Chapter 2 analyses this debate in more detail, with particular focus on the strengths and limitations of deterrence-by-punishment.

[67] Franklin Kramer, Robert Butler and Catherine Lotrionte, 'Cyber, Extended Deterrence, and NATO', *Atlantic Council*, (2016), last accessed on (09/09/2020), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf; Iftimie, 'NATO's Needed Offensive Cyber Capabilities', 1-4; Dorothy Denning, 'Rethinking The Cyber Domain and Deterrence', *Joint Forces Quarterly*, 77, (2015), 8-15. Denning argues the cyber domain is no different from other domains, meaning that cyber-deterrence works much like conventional deterrence.

[68] Matthew Crosston, 'World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope For Cyber Deterrence', *Strategic Studies Quarterly*, 5:1, (2011), 100-116.

[69] William Lynn III, 'Defending a New Domain - The Pentagon's Cyberstrategy', *Foreign Affairs*, 89, (2010), 97-108; Geers, 'The Challenge of Cyber Attack Deterrence', 301.

[70] Joseph Nye, 'Deterrence and Dissuasion in Cyberspace', *International Security*, 41:3, (2017), 44-71.

[71] Annegret Bendiek and Tobias Metzger, 'Deterrence Theory in the Cyber-century', *Informatik*, (2015), 558.

Chapter 2: The Utility of Offensive Cyber to NATO

Offensive cyber capabilities would likely help NATO achieve its two main purposes: deterring aggression and collective defence.[72] Specifically, this section focuses on using offensive cyber assets to deter *cyberattacks* via *deterrence-by-punishment*. This is for two reasons. First, NATO is far more likely to face cyber-incursions of the type deployed against Ukraine than a conventional attack.[73] This is because cyberattacks are currently relatively low risk for an attacker and can be used to subvert an Article 5 response. Second, Chapter 1 has shown that the question of using offensive cyber for deterrence-by-punishment is a lively and unresolved academic debate, thus demanding more analysis here. This chapter argues that a joint offensive cyber capability would likely improve NATO's cyber-deterrent posture, despite the severe criticism of cyber-deterrence-by-punishment in the literature. Next, this chapter analyses whether an integrated offensive cyber capability would assist NATO's collective defence and warfighting ability. This is a more straightforward argument, as it clearly would.

Joint Offensive Cyber Capabilities and Cyber Deterrence-by-Punishment

It is necessary to explain the limitations of NATO's current deterrence-by-denial policy to contextualise cyber deterrence-by-punishment. After all, one may ask: why not just bolster NATO's cyber defences? While defensive measures are absolutely essential for stopping attacks *that have already launched*, they are severely limited at deterring *potential* attacks. This probably explains why NATO does not mention 'cyber deterrence-by-denial' in its policy documents, but rather cyber-deterrence more broadly.[74] The main problem with deterrence-by-denial is that cyberattacks are very low cost for an aggressor, both in terms of the effort expended

[72] NATO, 'Deterrence and Defence'.
[73] Lewis, 'The Role of Offensive Cyber Operations in NATO's Collective Defence', 5.
[74] NATO, 'Deterrence and Defence'.

to launch an attack and the cost of penalties.[75] The existence of a huge black market offering everything from zero-day exploits to off-the-shelf services to conduct DDoS attacks facilitates the ease with which cyberattack technology can be acquired.[76] Meanwhile, the lack of an inspection regime and the infancy of international legal frameworks reduces the risk of penalties.[77] This gives aggressors little incentive to stop attacking, even in the face of strong defences. Meanwhile, defence in cyberspace is porous in nature.[78] Every system has vulnerabilities and exploiting them is only a matter of time, means and determination.[79] This permeability is a serious problem, because defenders must convince aggressors that an attack will have little to no effect for deterrence-by-denial to be effective.[80] NATO's deterrence-by-denial posture certainly makes attacks harder to conduct, but this has not deterred the hundreds of significant attacks it faces monthly. Clearly, a discussion over cyber deterrence-by-punishment is warranted.

The cyber deterrence-by-punishment that offensive weapons afford serves to *bolster* and *complement* deterrence-by-denial. This is because it threatens the imposition of costs where, in the absence of retaliation, there would be hardly any. In practice, retaliating might mean infecting an aggressor's systems with a worm to destroy files or deny services.[81] Deterrence-by-punishment faces severe criticism in the literature, for reasons that are addressed and countered later in this chapter.[82] This thesis acknowledges that *both* deterrence-by-denial and by-punishment face

[75] Bendiek and Metzger, 'Deterrence Theory in the Cyber-century', 562.
[76] Geers, 'The Challenge of Cyber Attack Deterrence', 302; Bendiek and Metzger, 'Deterrence Theory in the Cyber-century', 562.
[77] Geers, 'The Challenge of Cyber Attack Deterrence', 302.
[78] Patrick Morgan, 'Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm', in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, (Washington, DC: National Academies Press, 2010), pp. 55–76.
[79] Mariarosaria Taddeo, 'The Limits of Deterrence Theory in Cyberspace', *Philosophy & Technology*, 31:3, (2018), 346.
[80] Hideyuki Fujii, 'Deterrence by Resilience in Cyberspace', in *Cyber Defense: Policies, Operations and Capacity Building,* ed. Sandro Gaycken, (Amsterdam: IOS Press, 2019), p. 30.
[81] Lin, 'Offensive Cyber Operations and the Use of Force', 69-70.
[82] Bendiek and Metzger, 'Deterrence Theory in the Cyber-century', 558.

challenges of credibility.[83] However, their respective limitations *strengthen* the need for them to complement each other.

Discussing a cyber deterrence-by-punishment posture for NATO is nevertheless a very valid exercise. Principally, this is because many of the criticisms levelled against cyber-deterrence's credibility stem from unhelpful comparisons with Cold War-era nuclear deterrence.[84] Nuclear deterrence fails as soon as a single missile is launched because the weapons are enormously destructive. It is unhelpful to draw this comparison because the fallout from any cyberattack is much smaller than that of a nuclear strike. Cyberattacks are relatively low-impact, high-frequency events compared with high-impact, low-frequency nuclear attacks.[85] Rather, cyber-deterrence must work on the assumption that networks are *already* compromised and that deterrence is always failing.[86] Since *absolute* deterrence in cyberspace is not possible, this thesis agrees with Uri Tor and Lucas Kello's concept of 'cumulative deterrence' in cyberspace.[87] The aim of cumulative deterrence is to *minimize* the frequency of attacks and the damage inflicted on defended systems and infrastructure.[88] This is a far more realistic goal given the nature of cyberwarfare and the impossibility of absolute deterrence. Cyber deterrence-by-punishment is a very possible goal, as long as it is framed in cumulative deterrence terms.

[83] Clorinda Trujillo, 'The Limits of Cyberspace Deterrence', *Joint Forces Quarterly*, 75, (2014), 50; Fujii, 'Deterrence by Resilience in Cyberspace', p. 30; Geers, 'The Challenge of Cyber Attack Deterrence', 302.

[84] Martin Libicki, 'Cyberdeterrence and Cyberwar', *RAND Corporation*, (2009), xvi.

[85] James Lewis, 'Strategy After Deterrence', *Center for Strategic and International Studies*, (2020), last accessed on (09/09/2020), https://www.csis.org/analysis/strategy-after-deterrence.

[86] Bendiek and Metzger, 'Deterrence Theory in the Cyber-century', 558.

[87] Lucas Kello, *The Virtual Weapon and International Order*, (New Haven: Yale University Press, 2017), pp. 197-209; Uri Tor, 'Cumulative Deterrence' As A New Paradigm For Cyber Deterrence', *Journal of Strategic Studies*, 40:2, (2017), 92-117.

[88] Tolga, 'Principles of Cyber Deterrence and the Challenges in Developing a Credible Cyber Deterrence Posture', 18; Joe Burton, 'Cyber Deterrence: A Comprehensive Approach?', *NATO CCDCOE*, (2018), last accessed on (09/09/2020), https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf, 14; Tor, 'Cumulative Deterrence', As A New Paradigm For Cyber Deterrence', 93.

With this established, it is possible to set out this chapter's main argument: *that a joint offensive cyber capability would enhance the Alliance's cyber-deterrent posture*. There are three reasons for this. It would: improve intra-alliance knowledge transfer of cyber-intelligence gathering and cyber-sabotage techniques; help coordinate attacks and mitigate fratricide; accelerate decision-making and streamline response scenario planning.

First, NATO's cyber-deterrence would be more credible because a joint cyber capability would facilitate knowledge transfer between member states. For deterrence to be successful, NATO has to convince aggressors that it can retaliate against the *right* aggressor in a manner that imposes *unacceptable* costs. However, state and non-state actors, like the Fancy Bear cyber-espionage group likely associated with the Russian security services, know that the disaggregation of member states' cyber assets makes this harder to achieve.[89] The primary reason for this separation of effort is that intelligence on adversaries' cyber vulnerabilities is closely guarded by national intelligence agencies.[90] This intelligence is absolutely critical for effective cyberattacks, since it is necessary to understand the targeted systems in great detail.[91] The CyOC will not go far enough in fostering intelligence sharing, even though it aims to 'integrate cyber capabilities into NATO planning and operations'.[92] It is certainly a step forward, but of those states that have offered their cyber effects to NATO, France and America have clearly stated they will retain full control of their operations and capabilities.[93] This lack of joint operational authority poses a significant challenge, as

[89] Crowdstrike, 'Who is Fancy Bear (APT28)?', *Crowdstrike*, (2019), last accessed on (09/09/2020), https://www.crowdstrike.com/blog/who-is-fancy-bear/.

[90] Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', 6.

[91] Smeets, 'Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment', 400.

[92] NATO, 'The NATO Command Structure Factsheet', *NATO*, (2018), last accessed on (09/09/2020), https://www. nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/1802-Factsheet-NATO-CommandStructure_en.pdf.

[93] War on The Rocks, 'A Close Look At France's New Military Cyber Strategy', *War on The Rocks*, (2019), last accessed on (09/09/2020), https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/; CNBC, 'US to Offer Cyberwar Capabilities to NATO Allies', *CNBC*, (2018), last accessed on (09/09/2020), https://www.cnbc.com/2018/10/03/us-to-offer-cyberwar-capabilities-to-nato-allies.html.

it appears the centre will serve to coordinate rather than oversee operations.[94] It will prove very hard to achieve even this when members' capabilities vary greatly in their maturity and development. Whereas Germany is said to have thousands of 'information and cyber officers', other European states have hardly any.[95] Overall, NATO in its current state is not optimised for deterrence-by-punishment and the CyOC will do little to improve this.

Instead, pooling members' cyber-intelligence and cyber-sabotage expertise would encourage intra-alliance knowledge transfer. Knowledge transfer in organisations is the process through which one unit, like a department or division, is affected by the experience of another.[96] Empirical evidence suggests that interconnected organisations like franchises and chains hold comparative advantages over their autonomous counterparts, due to the ability to transfer knowledge between their constituent elements.[97]

This would apply to NATO in two ways. First, organisational integration of cyber-intelligence would facilitate knowledge transfer, as demonstrated by the preparations behind Stuxnet.[98] To design such a complex computer worm, the US National Security Agency (NSA) collaborated with Israel's counterpart, Unit 8200, largely because it had deep intelligence about operations at Iran's Natanz facility.[99]

[94] Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', 7.

[95] Max Smeets, 'Europe Slowly Starts to Talk Openly About Offensive Cyber Operations', *Council on Foreign Relations*, (2017), last accessed on (09/09/2020), https://www.cfr.org/blog/europe-slowly-starts-talk-openly-about-offensive-cyber-operations.

[96] Linda Argote and Paul Ingram, 'Knowledge Transfer: A Basis For Competitive Advantage In Firms', *Organizational Behavior and Human Decision Processes*, 82:1, (2000), 151.

[97] Ibid, 162.

[98] Smeets, 'Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment', 400.

[99] The New York Times, 'Obama Order Sped Up Wave of Cyberattacks Against Iran', *The New York Times*, (2012), last accessed on (09/09/2020), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

This was vital for the attack's success, because the individual control systems they targeted had unique configurations, making them harder to penetrate.[100]

Second, merging cyber-sabotage capabilities would similarly aid knowledge transfer. There are two types of knowledge required for cyber-sabotage operations. One type is explicit and can be transferred in a systematic manner, such as knowledge of how a SCADA system works or how to write code in a certain programming language.[101] The other, more significant type is *tacit* knowledge, which is difficult to transfer to another person by verbalising or writing it down.[102] This could include a hacker's accumulated experience or knowledge of a cyber command's implicit operational processes.[103] Tacit knowledge can be shared, but this is done by performance and learning by example.[104] A joint offensive cyber capability would provide an excellent opportunity for this to happen.[105] Both forms of knowledge transfer would be especially useful for 'upskilling' those NATO members that lack the advanced technical expertise in America, Britain, France and Germany. In practice, this would make acquiring cyberattack tools and training personnel easier and cheaper.[106] The importance of training technical personnel should not be underestimated, because all members are short of them but most lack the resources to attract them.[107] Pooling capabilities is one way of alleviating this pressure. In turn, the cumulative benefits of knowledge transfer would likely make it easier to launch retaliatory attacks against the right aggressor and impose unacceptable costs more

[100] Ibid; Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies*, 35:1, (2012), 19.
[101] Smeets, 'Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment', 401.
[102] Martin Davies, 'Knowledge – Explicit, Implicit and Tacit: Philosophical Aspects', in *International Encyclopaedia of the Social & Behavioral Sciences*, ed. James Wright, (New York: Elsevier, 2015), p. 74; Smeets, 'Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment', 401.
[103] Ibid.
[104] Davies, 'Knowledge – Explicit Implicit and Tacit', p. 74.
[105] Smeets, 'Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment', 401.
[106] James Lewis, 'Cyberspace and Armed Forces: The Rationale for Offensive Cyber Capabilities', *Australian Strategic Policy Institute*, (2016), last accessed on (09/09/2020), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/SI106_Cyberspace_armed-forces.pdf?8yAfEkjjYGgLpD0F3xF100AF5RHS.kPo, 4.
[107] Smeets, 'Europe Slowly Starts to Talk Openly About Offensive Cyber Operations'.

successfully. Overall, this would improve the credibility of a deterrence-by-punishment posture.

Furthermore, a joint capability would improve NATO's offensive cyber C2, improving attack coordination and mitigating fratricide. This is because NATO's 'volunteer' system and its CyOC mark a striking departure from the way it usually handles C2 of members' assets.[108] The NATO Force Structure dictates that conventional forces like ships and tanks come under the full operational control of an assigned NATO commander.[109] However, according to a retired USAF Colonel leading the implementation of NATO's 2017 cyber policy, the C2 problems inherent in the volunteer system make it 'far from ideal'.[110] This is because NATO commanders do not know the details of capabilities available to them, such as their legal consequences, impeding the decision-making process.[111] Commanders also want to know how using cyberweapons might conflict with other operations; without this they are left 'flying blind'.[112] Failing to coordinate operations can have far-reaching consequences. For instance, intelligence agencies' reconnaissance of target networks needs to be coordinated with cyber-sabotage operations, so they do not interfere with each other.[113] Disaggregated C2 can even result in fratricide on other allies' networks, because the distinction between internal and external security threats is much harder to ascertain in cyberspace than in the other four domains.[114] The CyOC is a step

[108] Rizwan Ali, 'NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons', *Foreign Policy*, (2017), last accessed on (09/09/2020), https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/.

[109] NATO, 'The NATO Force Structure', *NATO*, (2015), last accessed on (09/09/2020), https://www.nato.int/cps/en/natohq/topics_69718.htm.

[110] Ali, 'NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons'.

[111] Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', 6; Ali, 'NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons'.

[112] Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', 6; Ali, 'NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons'.

[113] Lewis, 'Cyberspace and Armed Forces: The Rationale for Offensive Cyber Capabilities', 4.

[114] Iftimie, 'NATO's Needed Offensive Cyber Capabilities', 2-4.

towards resolving this, but until a NATO commander has control over members' capabilities, these problems will not be fully resolved.

Additionally, a unified offensive cyber C2 structure would aid scenario planning and speed up decision-making. This is important, because NATO needs to streamline its current decision-making process in the cyber domain.[115] A single command would help members agree on appropriate forms of retaliation in cyberspace in different scenarios, bolstering the credibility of deterrence-by-punishment even further. Without a clear command structure, it is very difficult for the 30 NATO allies – who have different threat perceptions and suffer from a lack of cohesion – to agree on effective response scenarios in contingency planning.[116] As a case in point, Estonia is willing to strike back when attacked online, given its memory of the 2007 attack and its proximity to Russia.[117] However, Estonian officials do not know whether other allies will support them, validating some scholars' arguments that NATO needs to find common ground in cyber contingency planning.[118] The secrecy that shrouds allies' capabilities and the uncertainty surrounding cyber scenario planning might explain why offensive cyber effects do not feature in NATO's mission planning process.[119] This is not to say that NATO needs to *publicly* agree on a 'red line' in cyberspace that could trigger an Article 5 response. If anything, NATO's current strategic ambiguity is key for deterring attacks that fall just below a defined threshold.[120] However, unifying cyber C2 would help them carry out scenario planning behind closed doors, improving the Alliance's readiness. Speeding up the

[115] Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', 1.
[116] Ibid, 6.
[117] Patrick Tucker, 'How NATO Is Preparing to Fight Tomorrow's Cyber Wars', *Defense One*, (2017), last accessed on (09/09/2020), https://www.defenseone.com/technology/2017/10/how-nato-preparing-fight-tomorrows-information-wars/142084/.
[118] Ibid; Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', 7; Matthijs Veenendaal, Kadri Kaska and Pascal Brangetto, 'Is NATO Ready To Cross The Rubicon On Cyber Defence?', *NATO CCDCOE,* (2016), last accessed on (09/09/2020), https://www.ccdcoe.org/uploads/2018/10/NATO-CCD-COE-policy-paper.pdf, 6.
[119] Iftimie, 'NATO's Needed Offensive Cyber Capabilities', 2.
[120] Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', 2.

decision-making process is crucial given how long it can take to attribute and then launch a retaliatory attack.[121] Overall, streamlined scenario planning and decision-making, augmented by improved coordination of cyberattacks, would strengthen the credibility of deterrence-by-punishment. Although aggressors like Fancy Bear would not know when a certain threshold has been crossed, it would tilt their risk-benefit calculus knowing an attack could trigger a faster, well-coordinated retaliatory attack.

Cyber Deterrence-by-Punishment: Engaging with its Critics

Despite these benefits, it is worth reiterating the point made in Chapter 1: cyber deterrence-by-punishment is not a 'silver bullet' that solves the problems of deterrence-by-denial; rather, it faces many challenges. However, to demonstrate that a joint offensive cyber capability would nonetheless be a useful tool alongside defensive measures, it is necessary to engage with scholars' severe criticism of deterrence-by-punishment.

The main critique of deterrence-by-punishment is that it is hard to attribute cyberattacks. This reduces the credibility of deterrence because it is too difficult to tell which systems to retaliate against.[122] Nevertheless, though attribution is costly and time-consuming, it is possible.[123] On a technical level, malware's source code and programming style can be mapped against previous incidents.[124] In Iran, these forensics revealed similarities between Stuxnet and another virus developed by the NSA called Flame, intensifying accusations against US involvement in both tools.[125]

[121] Erik Gartzke and Jon Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', *Security Studies*, 24:2, (2015), 321; Bendiek and Metzger, 'Deterrence Theory in the Cyber-century', 562.

[122] Taddeo, 'The Limits of Deterrence Theory in Cyberspace', 344; Hunker, 'Cyber War and Cyber Power: Issues for NATO Doctrine', 5; Trujillo, 'The Limits of Cyberspace Deterrence', 5.

[123] Bendiek and Metzger, 'Deterrence Theory in the Cyber-century', 563.

[124] Ibid.

[125] The Washington Post, 'U.S., Israel Developed Flame Computer Virus To Slow Iranian Nuclear Efforts, Officials Say', *The Washington Post*, (2012), last accessed on (09/09/2020), https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html; Bendiek and Metzger, 'Deterrence Theory in the Cyber-century', 563.

Furthermore, anonymity in cyberspace is not as pervasive as critics make out, because attackers do make mistakes. For instance, the Chinese hacker group APT1 is recognisable for its sloppy re-use of social engineering tactics and specific infrastructure.[126] Additionally, attribution is facilitated by examining the history and politics surrounding an attack; in the case of Stuxnet, the tense relations between America, Israel and Iran narrowed down the list of likely sources.[127] What's more, Russia is increasingly likely to use its state security services to conduct attacks, instead of more anonymous but lower skilled non-state hackers.[128] This suggests that attacks from NATO's main adversary in cyberspace may become more traceable.

Most importantly, a joint offensive cyber capability would benefit NATO *precisely because* attribution is time consuming and costly. The quality of attribution is a function of available resources – the more there are, the more accurately one can attribute an attack.[129] Although pooling NATO's capabilities would not increase the quantity of resources available, it would improve *resource allocation* and thus allow NATO to 'do more with the same'.[130] In several countries, the growth of offensive cyber has already allowed for greater specialisation in cyber operations. US Cyber Command (USCYBERCOM) now has 133 teams, making it easier to dedicate teams to specific tasks.[131] This division of labour, enabled by pooling capabilities, would hopefully allow NATO to devote specialised units to cyber forensics. This would likely increase their output, facilitating timely and accurate attribution.

Another key criticism of deterrence-by-punishment is that it is hard to signal one's capabilities, because the secretive and 'single-use' nature of cyberweapons

[126] Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies*, 38:2, (2015), 22.
[127] Burton, 'Cyber Deterrence: A Comprehensive Approach?', 11.
[128] Michael Connell and Sarah Vogler, 'Russia's Approach to Cyber Warfare', *Center for Naval Analyses*, (2017), last accessed on (09/09/2020), https://apps.dtic.mil/sti/pdfs/AD1032208.pdf, 20.
[129] Rid and Buchanan, 'Attributing Cyber Attacks', 32.
[130] Smeets, 'Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment', 401-2.
[131] Ibid, 402.

means they cannot be paraded.[132] While it is true that cyberweapons' effects cannot be disclosed, critics are wrong to draw *direct* comparisons with nuclear weapons and assume that displaying force 'from the side-lines' is a necessary condition for cyber deterrence-by-retaliation.[133] This is because it is not necessarily the *only* form of signalling conducive to successful deterrence. Unlike nuclear weapons, cyberweapons can be used to signal intent and shape actors' behaviour through their *actual use*. For NATO, this would mean defining unacceptable behaviour through a campaign of persistent engagement: short, sharp rebukes over an extended period.[134] USCYBERCOM has already adopted a posture of 'persistent action… to deter aggression', by preventing and punishing attacks close to their origins.[135] It is too early to argue that NATO should adopt a similar signalling posture, because persistent engagement is still in its infancy and faces its own set of risks, like misperception and miscalculation.[136] Nobody, not even USCYBERCOM, yet knows whether persistent engagement will work.[137] Despite this, the fact that NATO's biggest member is experimenting with it presents an opportunity for the Alliance to learn from the US. If experience proves that persistent engagement largely works, the door is open for NATO to adopt a similar posture in future. Therefore, though signalling from afar in cyberspace is difficult, this may not actually matter as allies' cyber doctrine evolves.

A third criticism is that retaliatory cyberattacks can easily cause collateral damage and are dangerously escalatory. Since the distinction between internal and external networks is often blurred, attacks directed at a defender's network may spill

[132] Gartzke and Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', 322; Bendiek and Metzger, 'Deterrence Theory in the Cyber-century', 559; Trujillo, 'The Limits of Cyberspace Deterrence', 49-50.
[133] Bendiek and Metzger, 'Deterrence Theory in the Cyber-century', 558.
[134] James Lewis, 'Strategy after Deterrence'.
[135] USCYBERCOM, 'Achieve and Maintain Cyberspace Superiority', *USCYBERCOM*, (2018), last accessed on (09/09/2020), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.
[136] Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', *Journal of Cybersecurity,* 5:1, (2019), 11.
[137] Ibid.

over into external networks.[138] Adopting a persistent engagement approach will also pose increasing risks for escalation.[139] This is aggravated by the absence of international agreements determining unacceptable behaviour in cyberspace.[140] This dissertation does not dispute these criticisms; on the contrary, they *strengthen* the case for a joint-NATO offensive cyber capability. This is because one of the main solutions to these problems is increased control of cyber operations.[141] A joint capability would increase NATO members' control, because it would facilitate agreement on how to integrate offensive cyber effects into a Flexible Deterrent Options (FDO) package.[142] FDOs are meant to allow for a gradual increase of pressure in response to threats, limiting the chance of uncontrolled escalation.[143] Chapter 5 outlines how offensive cyber could be integrated into an FDO package in more detail. Leaving members to adhere to their own FDOs undermines the unity of NATO's response to an attack. Similarly, the extra control that centralised C2 offers would allow NATO to reduce the risk of cyberattacks causing collateral damage.[144] Though this risk cannot be eliminated entirely, joint C2 and standardised offensive cyber doctrine could add extra controls that seem unlikely to appear at the CyOC. For instance, doctrine could dictate that large attacks should only be launched against military networks; air defence systems are unlikely to be on the same network as hospitals, mitigating the chance of collateral damage.[145]

[138] Wyatt Hoffman and Ariel Levite, 'Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?', *Carnegie Endowment for International Peace*, (2017), last accessed on (09/09/2020), https://carnegieendowment.org/files/Brief-Cyber_Defense.pdf, 9; Geers, 'The Challenge of Cyber Attack Deterrence', 301.

[139] Taddeo, 'The Limits of Deterrence Theory in Cyberspace', 352.

[140] Bendiek and Metzger, 'Deterrence Theory in the Cyber-century', 564.

[141] Taddeo, 'The Limits of Deterrence Theory in Cyberspace', 350.

[142] Iftimie, 'NATO's Needed Offensive Cyber Capabilities', 3.

[143] Ibid.

[144] Lewis, 'Cyberspace and Armed Forces: The Rationale for Offensive Cyber Capabilities', 4; Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', 1.

[145] Lewis, 'Cyberspace and Armed Forces: The Rationale for Offensive Cyber Capabilities', 3.

Finally, critics argue that a joint cyber capability would trigger a cyber arms race by militarising the digital domain.[146] However, this is yet another misapplied comparison with nuclear deterrence. The difference is that Russia and China have *already* acquired many offensive cyber assets, by employing hacktivists, criminal syndicates and other advanced persistent threats.[147] Centralising a set of *existing* national capabilities is best seen as a step in military modernisation necessary to maintain the value of these capabilities, not an arms race.[148]

Joint Offensive Cyber and Collective Defence

The benefits of a joint offensive cyber capability for conventional collective defence are far easier to discern than cyber-deterrence. NATO could use it for tactical operations to support combat operations and shape the battlefield.[149] The most obvious scenario this could be used in is if NATO were attacked by Russia, the only state whose conventional forces pose a threat. Offensive cyber capabilities would be an important force multiplier in the event of a Russian attack on the Baltic states, where local force ratios would favour the attacker.[150] Battlefield NATO commanders could use cyber effects to disrupt Russian C2 networks or the software on advanced weapons, like surface-to-air missiles or fighter aircraft.[151] Anti-access/ area denial operations (A2/AD) like these seek to deny attackers the ability to bring their assets into a contested region and prevent them from operating freely within it.[152] Offensive cyber capabilities have already been used in this way to great effect. In 2007, the Israeli Air Force allegedly used the Suter computer program to conduct an airstrike against

[146] Trujillo, 'The Limits of Cyberspace Deterrence', 47-8.

[147] Connell and Vogler, 'Russia's Approach to Cyber Warfare', 27.

[148] Lewis, 'Cyberspace and Armed Forces: The Rationale for Offensive Cyber Capabilities', 3.

[149] Lewis, 'The Role of Offensive Cyber Operations in NATO's Collective Defence', 4.

[150] Kramer, Butler and Lotrionte, 'Cyber, Extended Deterrence, and NATO', 8-9.

[151] Lewis, 'The Role of Offensive Cyber Operations in NATO's Collective Defence', 4.

[152] Alison Russell, 'Strategic Anti-access/Area Denial in Cyberspace', *NATO CCDCOE*, (2015), last accessed on (09/09/2020), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7158475&casa_token=aYyp4LcV1B0AAAAA:0_xoO1wlkDtp6eWDedSgmUY_oyWBQSTkYmItuml272dqgnAbX5MlOcLr1IYASTcp-n1mJi52&tag=1, 154.

a nuclear reactor in Northern Syria.[153] This fed Syria's air defence systems a false-sky picture, allowing Israeli fighter jets to successfully bomb the reactor without being detected.[154] In many ways, cyber effects will become a basic necessity in conventional warfare. No modern air force would enter combat without electronic warfare (EW) capabilities; as cyber and EW merge into a single activity, air operations will *require* cyber support.[155] Overall, since cyberweapons can be so effective on the battlefield, they would clearly aid NATO's warfighting ability.

A *joint* capability would the best way to fulfil this role. The CyOC is hoping to coordinate battlefield effects in a similar way.[156] However, the secrecy of members' capabilities and the persistence of sovereign operational authority will make it harder for SACEUR to quickly decide whether and how to use cyberweapons. This would be detrimental in a hot war scenario, the rapid pace of which demands decisions to be made 'at the speed of relevance'.[157] Additionally, offensive cyberweapons depend heavily on force integration to be effective on the battlefield.[158] The greater the integration between conventional and cyber operations, the greater the multiplier effect achieved – as proved by Israel's highly coordinated airstrike.[159] However, it seems the current volunteer system is lacking in this regard. A senior NATO official has acknowledged the Alliance needs to get better at aligning its cyber assets with its Enhanced Forward Presence (EFP) in the Baltics as part of an A2/AD strategy.[160] This means it needs to improve coordination with the EFP's graduated response plans and practise battlefield cyberattacks in a more realistic way during exercises.[161] To this

[153] Max Smeets, 'The Strategic Promise of Offensive Cyber Operations', *Strategic Studies Quarterly*, 12:3, (2018), 96.
[154] Ibid.
[155] Lewis, 'The Role of Offensive Cyber Operations in NATO's Collective Defence', 3.
[156] Reuters, 'NATO Cyber Command to be Fully Operational in 2023'.
[157] Jamie Shea, 'How is NATO Meeting the Challenge of Cyberspace?', *Prism*, 7:2, (2017), 21.
[158] Smeets, 'The Strategic Promise of Offensive Cyber Operations', 98.
[159] Ibid, 99.
[160] Shea, 'How is NATO Meeting the Challenge of Cyberspace?', 21.
[161] Ibid.

end, the improved C2, knowledge transfer and resource allocation that a joint cyber capability offers would augment not just cyber-deterrence but collective defence too.

Chapter 3: Would a Joint Capability be Practical to Establish?

Though a joint offensive cyber capability may be desirable, it would be very difficult to establish in the short-term. This is for two main reasons. First, it would be highly politically sensitive for member states to set it up. Second, national intelligence agencies are highly secretive about their cyber-warfare techniques, making their integration on a multilateral level very difficult.

There are several reasons why establishing a combined offensive cyber capability would face political obstacles. The most important of these is that the unpredictability of cyberweapons' effects entails potentially profound political risk on the unilateral level, let alone the multilateral level.[162] As a case in point, the Obama Administration rejected nearly all proposed cyber responses to Russian incursions into the Democratic National Committee's communications in 2016.[163] It decided they would be ineffective, escalatory, or would prematurely expose US offensive cyber capabilities and compromise long-term intelligence gathering efforts.[164] Though Chapter 2 is right to argue that a pooled capability would help mitigate many of cyberweapons' problems in the *long-term*, much still remains unclear regarding their impact, unintended effects, escalatory risks and political consequences *at the moment*.[165] This uncertainty makes political leaders reluctant either to use cyberweapons or to commit to ambitious new offensive cyber policy objectives.[166] Therefore, although there are many existing cyber *defence* agreements at national and regional levels, such as the 2016 NATO-EU Technical Arrangement on Cyber Defence,

[162] Lewis, 'The Role of Offensive Cyber Operations in NATO's Collective Defence', 7-8.

[163] Shea, 'How is NATO Meeting the Challenge of Cyberspace?', 12.

[164] Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', 4; Shea, 'How is NATO Meeting the Challenge of Cyberspace?', 12.

[165] Matthijs, Kaska and Brangetto, 'Is NATO Ready To Cross The Rubicon On Cyber Defence?', 7; Lewis, 'The Role of Offensive Cyber Operations in NATO's Collective Defence', 8.

[166] Veenendaal, Kaska and Brangetto, 'Is NATO Ready To Cross The Rubicon On Cyber Defence?', 7; Lewis, 'The Role of Offensive Cyber Operations in NATO's Collective Defence', 8.

political consensus among allies is lacking on whether they should be expanded to incorporate the collective use of offensive cyber capabilities.[167]

Additionally, publicly announcing a joint offensive cyber capability is politically sensitive, particularly at a time when NATO is badly divided.[168] One possible explanation for this sensitivity is that there is neither the expectation nor intent among political leaders for NATO to engage in major military operations, reducing the need to plan for using cyberattacks.[169] Furthermore, NATO is heavily divided over two main issues completely separate from the cyber domain. First, the Alliance is plagued by the East/ South divide. This refers to friction between members over whether NATO should focus east, towards a revanchist Russia, or south, towards the Middle East and Mediterranean.[170] Recently, deteriorating NATO-Turkey relations have epitomised the East/ South divide. Bordering the volatile Syrian civil war, Turkey accuses the Alliance of not taking its security concerns seriously.[171] In late 2019, Ankara blackmailed NATO by refusing to approve military plans for the Baltic States and Poland in return for more political support in Syria.[172] That Turkey would block plans aimed at countering Russian aggression in the East raises significant doubts that it would support a joint offensive cyber capability, given that Russia is NATO's largest adversary in cyberspace.[173] Second, a key theme over NATO's last four years has been Donald Trump's criticism that other members states

[167] Iftimie, 'NATO's Needed Offensive Cyber Capabilities', 4.
[168] Lewis, 'The Role of Offensive Cyber Operations in NATO's Collective Defence', 10.
[169] Ibid.
[170] Alina Inayeh, Ozgur Unluhisarcikli and Michal Baranowski, 'Avoiding the East-South Divide Ahead of the NATO Summit', *The German Marshall Fund of the United States,* (2016), last accessed on (09/09/2020), https://www.gmfus.org/blog/2016/06/08/avoiding-east-south-divide-ahead-nato-summit.
[171] EURACTIV, 'Turkey Not Backing Down in NATO Defence Plans Dispute – Source', *EURACTIV*, (2019), last accessed on (09/09/2020), https://www.euractiv.com/section/defence-and-security/news/turkey-not-backing-down-in-nato-defence-plans-dispute-source/.
[172] Rachel Ellehuus, 'Turkey and NATO: A Relationship Worth Saving', *Center for Strategic and International Studies*, (2019), last accessed on (09/09/2020), https://www.csis.org/analysis/turkey-and-nato-relationship-worth-saving.

are not meeting the Alliance's 2% of GDP defence spending requirement.[174] Consequently, Trump has downgraded US contributions to NATO; in July he decided to withdraw 12,000 US troops from Germany in response to Berlin's failure to meet spending targets.[175] Should he win this year's presidential election, US support for a joint cyber capability would likely be sorely lacking for the next four years. Both these divisions have a good chance of overshadowing attempts to establish a joint cyber capability.

Despite these problems, it would not be impossible to overcome such political obstacles. First, these political hurdles do not rule out a debate concerning the establishment of a shared capability sometime in the future. The expiration date of NATO's current defence-limited policy appears due, especially as smaller members like Norway and The Netherlands have declared ambitions to develop offensive cyber capabilities, or have already deployed them as part of military operations.[176] NATO's declaration that it is not seeking a joint offensive cyber capability does not mean it is off the table forever. It may be driven to acquire one out of necessity, a key theme in the Alliance's history. When NATO was first founded, members did not think they needed a joint command structure, instead relying on Regional Planning Groups to perform disaggregated C2.[177] Nonetheless, the outbreak of the Korean War in 1950 raised fears that NATO's defence posture in Europe was inadequate.[178] Consequently, the Alliance shifted towards an integrated military command structure with an

[174] The Economist, 'NATO Members' Promise of Spending 2% of Their GDP on Defence is Proving Hard to Keep', *The Economist*, (2019), last accessed on (09/09/2020), https://www.economist.com/special-report/2019/03/14/nato-members-promise-of-spending-2-of-their-gdp-on-defence-is-proving-hard-to-keep.
[175] BBC News, 'US to Withdraw 12,000 Troops from Germany in 'Strategic' Move', *BBC News*, (2020), last accessed on (09/09/2020), https://www.bbc.co.uk/news/world-us-canada-53589245.
[176] Veenendaal, Kaska and Brangetto, 'Is NATO Ready To Cross The Rubicon On Cyber Defence?', 7; Lilly Muller, 'Military Offensive Cyber-Capabilities: Small-State Perspectives', *NUPI Policy Brief*, (2019), last accessed on (09/09/2020), https://nupi.brage.unit.no/nupi-xmlui/handle/11250/2583385, 2.
[177] SHAPE, '1949-1952: Creating A Command Structure for NATO', *SHAPE*, (2020), last accessed on (09/09/2020), https://shape.nato.int/page14612223.aspx.
[178] Ibid.

overall commander for NATO forces.[179] Further to this, integrating politically sensitive and secretive capabilities is not new to the Alliance. The Allied Joint Doctrine for the Conduct of Operations covers the use of special forces, acknowledging they employ 'specialised techniques' and that their operations 'might be executed where significant political risk exists'.[180] This approach could serve as a basis for joint cyber operations. At the least, it reflects NATO's adaptability and ability to develop doctrine for non-conventional forces.[181] Therefore, though the political obstacles are significant, they can be overcome.

Nevertheless, the largest barrier to a joint cyber capability is national intelligence agencies' tendency to keep their activities in cyberspace highly classified.[182] As Chapter 2 discussed, effective cyberattacks are utterly dependent on excellent intelligence.[183] Members have significantly stepped up intelligence-sharing over the last two decades. They established the NATO Intelligence Fusion Centre in 2006, the Joint Intelligence, Surveillance and Reconnaissance initiative in 2012 and the Joint Intelligence and Security Division (JISD) in 2017. The JISD's first Assistant Secretary General, Arndt Freytag von Loringhoven, says it has fostered a new culture of intelligence cooperation, increased efficiency and has helped avoid the duplication

[179] Ibid.

[180] NATO, 'AJP-3 Allied Joint Doctrine for the Conduct of Operations', *NATO*, (2019), last accessed on (09/09/2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf.

[181] Veenendaal, Kaska and Brangetto, 'Is NATO Ready To Cross The Rubicon On Cyber Defence?', 7.

[182] Burton, 'Cyber Deterrence: A Comprehensive Approach?', 6; Lucas Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security*, 38:2, (2013), 10; Artur Gruszczak, 'NATO's Intelligence Adaptation Challenge', *GLOBSEC*, (2018), last accessed on (09/09/2020), https://www.globsec.org/wp-content/ uploads/2018/03/NATO%E2%80%99s-intelligence-adaptation-challenge.pdf, 7.

[183] Smeets, 'Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment', 400.

of effort.[184] Notably, he claims this new fusion of intelligence has 'positioned the JISD to contend effectively with the… cyber… threats increasingly confronting NATO'.[185]

However, von Loringhoven's optimism glosses over the great difficulty of intra-Alliance intelligence sharing. Divulging secret information is a trade-off between trusting a partner enough to share information that could endanger one's own source against the benefits of doing so.[186] Therefore, national agencies are reluctant to share it with international organisations, instead preferring bilateral cooperation on a case-by-case basis.[187] It is shared between states with closely aligned interests, mutual trust and good diplomatic relations, as seen in the Anglo-American UKUSA Agreement.[188] The exclusive 'Five Eyes' Alliance this evolved into is a rare example of multilateral intelligence sharing, involving NATO members America, Canada and the UK. These agreements tend to be more concerned with the *security* of the intelligence shared rather than its content, due to concerns over how other states will circulate the information.[189] Accordingly, wider intelligence cooperation within NATO would be much harder to achieve, primarily because many states do not share strong levels of trust, common interests and diplomatic relations with each other. For instance, France remains unsympathetic to intelligence integration in *any* multilateral environment, preferring strategic autonomy.[190] This is compounded by an uneasy relationship with the Alliance, with President Emmanuel Macron calling it 'brain

[184] Arndt Freytag von Loringhoven, 'A New Era for NATO Intelligence', *NATO Review*, (2019), last accessed on (09/09/2020), https://www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html.

[185] Ibid.

[186] Jan Ballast, 'Trust (in) NATO: The Future of Intelligence Sharing Within the Alliance', *NATO Defence College*, (2017), last accessed on (09/09/2020), https://rieas.gr/images/rieasnews/NATOarticle17.pdf, 2.

[187] Ibid, 2-3.

[188] James Walsh, *The International Politics of Intelligence Sharing*, (New York: Columbia University Press, 2009), pp. 37-9; Ballast, 'Trust (in) NATO: The Future of Intelligence Sharing Within the Alliance', 3.

[189] Richard Aldrich, 'Transatlantic Intelligence and Security Cooperation', *International Affairs*, 80:4, (2004), 737.

[190] Ballast, 'Trust (in) NATO: The Future of Intelligence Sharing Within the Alliance', 12.

dead' in 2019.[191] Furthermore, some allies fear that if countries with lower resilience are infiltrated, they could possibly compromise sensitive information shared between members.[192] Consequently, apprehension about Italy's weak cyber systems hinders allies' propensity to share with Rome, since the potential for leaks undermines their trust.[193]

These concerns have resulted in a division between those member states that possess more advanced intelligence assets and those that do not. The former have been resisting serious intelligence integration, while the latter – including Belgium and The Netherlands – have even pressed for a CIA-style European agency.[194] So far, NATO's more powerful members have successfully repelled such initiatives. Following the 2015 Paris terror attacks, Belgian Prime Minister Charles Michel proclaimed the need for a 'European CIA'.[195] Nonetheless, German Interior Minister Thomas de Maizière shot this proposal down, claiming that 'I cannot imagine we will be willing to give up our national sovereignty'.[196]

Unsurprisingly, NATO's own collaborative efforts to date have also been heavily limited by national agencies' desire for secrecy and autonomy. Pushback against greater transparency is especially strong on the part of the US, which owns a large share of NATO's intelligence capabilities.[197] Upon von Loringhoven's arrival at his JISD post, his Deputy, US Brigadier General Paul Nelson, told him that he would

[191] The Economist, 'Emmanuel Macron Warns Europe: NATO is Becoming Brain-dead', *The Economist*, (2019), last accessed on (09/09/2020), https://www.economist.com/europe/2019/11/07/emmanuel-macron-warns-europe-nato-is-becoming-brain-dead.

[192] Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', 6.

[193] Keenan Mahoney, Joshua Rovner, Nemanja Mladenovic, Salvador Molina, Adam Scher, Selma Stern and Christopher Zoia, 'NATO Intelligence Sharing in the 21st Century', *Columbia School of International and Public Affairs*, (2017), 38-9.

[194] John Nomikos, 'A European Intelligence Service for Confronting Terrorism', *International Journal of Intelligence and CounterIntelligence*, 18:2, (2005), 192; Ballast, 'Trust (in) NATO: The Future of Intelligence Sharing Within the Alliance', 5.

[195] Giulia Paravicini, 'Europe's Intelligence 'Black Hole', *Politico*, (2015), last accessed on (09/09/2020), https://www.politico.eu/article/europes-intelligence-black-hole-europol-fbi-cia-paris-counter-terrorism/.

[196] Ibid.

[197] Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', 6.

not have access to all US intelligence, but NATO releasable information only.[198] Such secrecy is a big practical obstacle to a joint offensive cyber capability. Although it is justified, elevating America's role in Alliance cyber policy without increasing transparency would likely limit the tactical and strategic effectiveness of a combined offensive cyber capability.[199] NATO's intelligence fusion efforts have suffered from other, less important problems too. Different languages, cultures and infrastructures have proved to be structural constraints, while battlefield commanders have criticised the intelligence provided for lacking the strategic dimension.[200] For instance, Lieutenant-General Mark Hertling judged NATO's information on Islamic State too narrow and target-oriented, thus missing the bigger picture.[201]

Overall, the establishment of a joint capability would face some serious practical problems, both when confronting NATO's internal politics and national intelligence agencies' clandestine modus operandi. There would be significant legal hurdles to overcome too, which Chapter 4 discusses in more detail.

[198] Ballast, 'Trust (in) NATO: The Future of Intelligence Sharing Within the Alliance', 9.

[199] Arts, 'Offense As the New Defense: New Life for NATO's Cyber Policy', 6.

[200] Claudia Bernasconi, 'NATO's Fight Against Terrorism: Where Do We Stand?', *NATO Defence College*, 66, (2011), 5; Ballast, 'Trust (in) NATO: The Future of Intelligence Sharing Within the Alliance', 4, 8.

[201] Ibid, 8.

Chapter 4: Cyber Deterrence-by-Punishment and International Law

When discussing the establishment of a joint cyber capability, it is vital to take considerations of international law into account. This is because it is now generally held that international law does apply in cyberspace, while NATO has made it clear that adherence to it must be guaranteed when incorporating cyber effects.[202] Nevertheless, this is not straightforward. The Euro-Atlantic legal debate has shifted to *how* international law applies to cyberspace, because the absence of established norms and state practice makes this a very uncertain field.[203] There is little consensus on how international law, primarily the UN Charter, applies in cyberspace.[204] Therefore, this chapter outlines some of the key legal problems and grey areas NATO would face in the following three areas: first, in justifying the launch of retaliatory cyberattacks (hereby *jus ad bellum*); second, in abiding by international law when using cyber effects (hereby *jus in bello*); third, in integrating sovereign capabilities into a joint command in the first place. The issues and considerations outlined are not exhaustive, but are intended to give a sense of the legal challenges that would need to be overcome.

With regard to *jus ad bellum*, NATO would be justified in launching retaliatory cyberattacks in certain scenarios. Whether it does so as part of an Article 5 response would of course be a political decision made by the North Atlantic Council (NAC). The NAC's chosen response will doubtless be based on the *effects* of the attack launched against NATO, because the spectrum of possible cyber effects is so wide.[205]

[202] CCDCOE, 'Trends in International Law for Cyberspace', *CCDCOE*, (2019), last accessed on (09/09/2020), https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf, 1; Davis, 'NATO In The Cyber Age: Strengthening Security & Defence, Stabilising Deterrence', 9.

[203] CCDCOE, 'Trends in International Law for Cyberspace', 1; Lin, 'Offensive Cyber Operations and the Use of Force', 73.

[204] Mark Sexton, 'UK Cybersecurity Strategy and Active Cyber Defence – Issues and Risks', *Journal of Cyber Policy,* 1:2, (2016), 229.

[205] Lin, 'Offensive Cyber Operations and the Use of Force', 72.

The more destructive the effect, the more legal clarity there is on whether is constitutes an armed attack. At the clearer end of the spectrum, it is now generally believed that a cyberattack resulting in the destruction of physical property, injury or the loss of life constitutes a use of force under the UN Charter, Article 2(4).[206] In such scenarios, states are free to choose appropriate means to compel the incriminating actor to desist, including cyberattacks.[207] According to researchers at NATO's CCD CoE, their analysis indicates that reverting to countermeasures has been validated several times by the International Court of Justice.[208] Further along the spectrum, it also seems to be accepted that a cyber operation falling below the 'use of force' threshold could still be illegal, since it might violate the prohibition on intervention in international law.[209]

However, since the advent of cyber operations, states and scholars have struggled to define the threshold at which an act becomes a 'use of force'.[210] Attacks with grave consequences that *do not* damage property or life raise the biggest questions about what constitutes 'use of force'. This might include a gradual cyberattack on a stock exchange that causes great economic loss over time.[211] Though economic fallout can cause deaths, the causal chain is very indirect over an extended period, while the key question is: how much economic loss constitutes a 'use of

[206] Heather Dinniss, *Cyber Warfare and the Laws of War*, (Cambridge: Cambridge University Press, 2012), p. 74; CCDCOE, 'Trends in International Law for Cyberspace', 2.

[207] Ibid; Rod Thornton and Marina Miron, 'Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom', *Journal of Cyber Policy,* 4:2, (2019), 264; Michael Schmitt, 'The Law of Cyber Warfare: Quo Vadis', *Stanford Law and Policy Review,* 25, (2014), 281; Pascal Brangetto, Tomáš Minárik and Jan Stinissen, 'From Active Cyber Defence to Responsive Cyber Defence: A Way for States to Defend Themselves – Legal Implications', *NATO Legal Gazette,* 35, (2014), 22.

[208] Siim Alatalu, 'One Year After Warsaw: The Growing Need for a NATO Cyber Command', *NATO CCDCOE*, (2017), last accessed on (09/09/2020), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8167513&casa_token=QkFD97XIVmgAAAAA:tPF8ETfDvqcdXmHmq2ON76rB8s5lJBNoqHjuEixuSfbkyjBvfCw9qzGKOMbNw4hCeQ8FYo0B, 63.

[209] Thornton and Miron, 'Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom', 264; Brangetto, Minárik and Stinissen, 'From Active Cyber Defence to Responsive Cyber Defence', 22.

[210] Michael Schmitt, 'The Law of Cyber Targeting', *Naval War College Review*, 68:2, (2015), 3; Schmitt, 'The Law of Cyber Warfare: Quo Vadis', 279.

[211] Lin, 'Offensive Cyber Operations and the Use of Force', 75; Schmitt, 'The Law of Cyber Targeting', 4.

force'?[212] Difficult questions like these are important, because reaching greater international consensus on whether self-defence is justified requires a common understanding on the difference between nefarious economic activity and 'true' cyberattacks.[213] This consensus is proving difficult to create.[214] There are further legal issues that complicate the question of whether to launch a retaliatory attack. First, it is a moot point whether or not a cyberattack launched by a non-state actor justifies self-defence under UN Article 51.[215] Though there is general consensus that it *could*, the absence of tangible evidence this has yet happened means there is no legal precedent for it.[216] Russia and China pose particular difficulty in this regard, because they often sponsor non-state actors to carry out cyberattacks on their behalf.[217] Moscow and Beijing can simply claim patriotic citizens are to blame, without collusion from the state.[218] Second, even though a joint cyber capability would likely improve attribution, this may not always be enough in the eyes of international law. NATO would have to be absolutely sure it knew who launched an attack, because correct attribution helps a defender justify their decision to retaliate.[219] Consequently, the problems raised by these legal grey zones shows that it might often be very difficult to determine whether launching joint, retaliatory cyberattacks is appropriate in certain circumstances.

Assuming NATO decides it has legal grounds for launching a retaliatory cyberattack, the next stage is making sure this strike abides by *jus in bello*. There is

[212] Lin, 'Offensive Cyber Operations and the Use of Force', 75.
[213] Thornton and Miron, 'Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom', 268.
[214] Ibid.
[215] Sexton, 'UK Cybersecurity Strategy and Active Cyber Defence – Issues and Risks', 229.
[216] Laurie Blank, 'International Law and Cyber Threats from Non-state Actors', *US Naval War College International Law Studies*, 89, (2013), 415; Sexton, 'UK Cybersecurity Strategy and Active Cyber Defence – Issues and Risks', 229.
[217] Sigholm, 'Non-state Actors in Cyberspace Operations', 16.
[218] Hunker, 'Cyber War and Cyber Power: Issues for NATO Doctrine', 5.
[219] Taddeo, 'The Limits of Deterrence Theory in Cyberspace', 342; Thornton and Miron, 'Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom', 268.

now widespread agreement that International Humanitarian Law (IHL) – the law regulating the conduct of war – applies in its entirety to cyber operations conducted during an armed conflict.[220] The most important factor NATO has to consider is that its own cyberattacks remain lawful in accordance with the principles of distinction and proportionality.[221] The former refers to the distinction between military and civilian targets; it is a violation of IHL to conduct cyber operations intended to kill members of the civilian population.[222] The latter means that a response in cyberspace should be proportional to the injury suffered in the attack.[223] Meanwhile, a joint cyber capability may even *help* NATO abide by IHL should a cyber response promise less collateral damage than a kinetic one. In a hot war scenario, a cyberattack on a railway yard in a built up area would probably entail much less risk of collateral damage than an airstrike. In this scenario, NATO would be *obligated* by IHL to use the cyber option to minimise incidental civilian harm.[224] Overall, compared with the legal uncertainties of cyber *jus ad bellum*, it is clear that IHL does give NATO more clearly defined legal limits to operate within once hostilities commence.

Nonetheless, significant challenges remain with regard to *jus in bello* and cyberweapons. First, distinguishing between military and civilian targets is sometimes hard, because so many military functions and systems rely on civilian technology.[225] Although Chapter 2 gave the example of air defence networks, which have little crossover with civilian networks, many other targets are more complicated. Large amounts of military communications are still sent across civilian networks, while civilian websites can be used to coordinate military operations.[226] For instance,

[220] Schmitt, 'The Law of Cyber Targeting', 2.

[221] Smeets, 'Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment', 399; Geers, 'The Challenge of Cyber Attack Deterrence', 301; Sexton, 'UK Cybersecurity Strategy and Active Cyber Defence – Issues and Risks', 232.

[222] Schmitt, 'The Law of Cyber Targeting', 4.

[223] Sexton, 'UK Cybersecurity Strategy and Active Cyber Defence – Issues and Risks', 231.

[224] Schmitt, 'The Law of Cyber Targeting', 14-15.

[225] Schmitt, 'The Law of Cyber Warfare: Quo Vadis', 289.

[226] Heather Dinniss, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives', *Israel Law Review*, 48:1, (2015), 48.

Kurdish militias in Syria used Google Earth to coordinate American airstrikes on Islamic State positions.[227] Although civilian technologies used for military purposes unquestionably qualify as military objectives in times of war, they may still not qualify as legitimate targets if there is a risk of excessive collateral damage.[228] Thus, cyberwarfare exacerbates the long-standing debate over the definitions of military and civilian targets.[229]

Second, it can be very difficult to launch a proportional cyber response, for several reasons. If Russia launched a cyberattack on a member state's banks, as it did against Estonia, IHL would prevent NATO from launching commensurate attacks on Russian banks, because they are clearly civilian targets.[230] Attacking a different target to achieve similar effects would be very hard to perform. Additionally, before launching a retaliatory cyberattack, it is difficult to anticipate whether its likely collateral damage will be excessive in relation to the anticipated military advantage gained.[231] As Stuxnet demonstrated, even exceptionally well-executed cyberattacks can spread in unpredictable ways.[232] If a retaliatory strike did unintentionally contravene the principles of proportionality or distinction, it would be extremely difficult to hold NATO to account. If NATO breaches IHL, its constituent members are held accountable in international courts and tribunals.[233] However, it is very hard for victims to determine exactly which state is responsible because they lack mission-

[227] Tim Fernholz, 'How Google is Fighting ISIL in Syria', Quartz, (2015), last accessed on (09/09/2020), https://qz.com/476882/how-google-is-fighting-isis-in-syria/.

[228] Schmitt, 'The Law of Cyber Targeting', 9.

[229] Ibid.

[230] Rain Ottis, 'Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective', *NATO CCDCOE*, (2008), last accessed on (09/09/2020), https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf, 1; Thornton and Miron, 'Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom', 269.

[231] Schmitt, 'The Law of Cyber Targeting', 16.

[232] The New York Times, 'Obama Order Sped Up Wave of Cyberattacks Against Iran'.

[233] Nachama, Rosen, 'How are Multinational NATO Operations Responsible for International Humanitarian Law Violations', *Fletcher Forum of World Affairs,* 37:3, (2013), 167.

specific knowledge, while NATO's documents are mostly classified.[234] The highly secretive nature of cyber operations would likely aggravate this.

Finally, it would likely be very challenging to pool members' sovereign capabilities in the first place, because they currently abide by different legal codes in cyberspace. This is even posing a problem at the CyOC. According to Eneken Tikk of the Cyber Policy Institute in Finland, the legal 'elephant in the room' at Mons is bringing national realities and strategic ambitions together.[235] The starkest example of this problem is different member's legal conceptions of sovereignty in cyberspace. Although France perceives *any* penetration of its networks as a violation of sovereignty, the UK has instigated a lively legal debate by stating that it *does not* recognise sovereignty in cyberspace at all.[236] Moreover, the UK actually accepts that it cannot entirely conform to the laws of armed conflict when using offensive cyber in a deterrence capacity.[237] It seems it would be very hard for NATO to follow international law if its own members admit they cannot. Meanwhile, with regard to *jus in bello*, the US labels war-sustaining objects, such as munitions factories, as military objectives susceptible to lawful attack.[238] However, most other states do not adopt the US approach, most likely because attacking these targets risks infringing on the principles of proportionality and distinction.[239]

[234] Ibid, 168.

[235] EURACTIV, 'NATO Sees New Cyber Command Centre by 2023 as Europe Readies for Cyber Threats', *EURACTIV*, (2018), last accessed on (09/09/2020), https://www.euractiv.com/section/defence-and-security/news/nato-sees-new-cyber-command-centre-by-2023-as-europe-readies-for-cyber-threats/.

[236] Jeremy Wright, 'Cyber and International Law in the 21st Century', *UK Government*, (2018), last accessed on (09/09/2020), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; Mark Pomerleau, 'What is 'Sovereignty' in Cyberspace? Depends Who You Ask', *Fifth Domain*, (2019), last accessed on (09/09/2020), https://www.fifthdomain.com/international/2019/11/21/what-is-sovereignty-in-cyberspace-depends-who-you-ask/; CCDCOE, 'Trends in International Law for Cyberspace', 5.

[237] Thornton and Miron, 'Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom', 270.

[238] Schmitt, 'The Law of Cyber Targeting', 9-10.

[239] Ibid, 9.

Overall, NATO would face three very tough legal challenges if it were to form a joint offensive cyber capability. It would have to navigate the uncertainties of *jus ad bellum*, before selecting targets judiciously in accordance with *jus in bello*. Plus, to even establish the capability, it would have to iron out some of its members' key legal disagreements. This would not be easy and it would be unrealistic to hope to establish a joint capability in the short-term. However, it could be possible long-term, as Chapter 5 elaborates.

Chapter 5: Recommendations

The last three chapters demonstrate that a joint offensive cyber capability would likely improve NATO's cyber-deterrent posture and would certainly improve its collective defence. However, they also show that it is not a silver bullet and that establishing a joint capability would face serious political and legal obstacles. In light of these findings, this chapter makes the following recommendations.

Recommendation 1: NATO should look to acquire a joint offensive cyber capability in future, as part of an FDO ladder that combines offensive and defensive options

Creating a combined offensive cyber capability should be a long-term aim, although it is currently unrealistic in the face of practical and legal problems. As cyberattacks against the Alliance become increasingly frequent and destructive, a deterrence-by-punishment posture would complement and build upon the current strategy of denial.[240] Pooling members' assets would be the best way to achieve this and to provide a battlefield capability. As well as improving intra-alliance knowledge transfer, offensive cyber C2 and scenario planning, it would help overcome the problems of attribution and escalation in cyberspace. However, it would not solve these problems, nor the legal obstacles to the use of cyberweapons. NATO will find itself in plenty of situations where retaliation in cyberspace is either too uncertain, unnecessary or illegal. Main adversaries Russia and China know this, so NATO needs other options to maintain the credibility of deterrence-by-punishment. A joint cyber capability should be seen as another tool, alongside other measures like sanctions.[241]

They should be introduced as one rung in a ladder of escalating options, as per the FDOs mentioned in Chapter 2. This would allow for a gradual increase of pressure in the cyber domain, hopefully limiting the scope and intensity of conflict.[242] At the

[240] NATO, 'Cyber Defence'.
[241] Bendiek and Metzger, 'Deterrence Theory in the Cyber-century', 562.
[242] Iftimie, 'NATO's Needed Offensive Cyber Capabilities', 3.

lower end of the spectrum, NATO could enact defensive measures and increase readiness by conducting cyber exercises or deploying its existing Cyber Rapid Reaction teams to defend critical infrastructure.[243] Once again, it is important to highlight that cyber defence should remain the bedrock of NATO's strategy.[244] Pursuing an offensive capability should not detract from this, but should complement it. As hacks increase in severity, NATO could in increasing order: make official statements addressing violations of international law; impose political or economic sanctions; conduct offensive cyber operations against the source of an attack; and finally, trigger Article 5, using offensive cyber assets for collective defence.[245] Integrating a joint offensive cyber capability into an FDO package like this would also align well with the cumulative deterrence mentality necessitated by cyberwarfare. Possessing other response options would help NATO minimise the frequency and damage of attacks that come at differing levels of severity. For instance, it is probably best to focus on bolstering cyber defence to counter China's cyber-espionage efforts, because this sort of activity is at the lower end of the threat spectrum.[246]

It will be some time before NATO can realistically acquire a joint capability; it may never be able should intelligence agencies remain so intransigent. Nevertheless, the Alliance should take measures now to begin to overcome the obstacles mentioned in the previous three chapters. This is vital, because surmounting challenges as great as these will take time. Furthermore, if cyberattacks become unbearably crippling, NATO may find itself in a position where it is forced to adopt a deterrence-by-punishment stance and a joint offensive capability *out of necessity*. This is not fantastical, as the Korean War's impact on the formation of the NATO Command Structure shows. NATO must prepare the ground for such a move accordingly. Some of the most important measures it should take are as follows:

[243] Ibid.

[244] NATO, 'Cyber Defence'.

[245] Iftimie, 'NATO's Needed Offensive Cyber Capabilities', 3.

[246] Hunker, 'Cyber War and Cyber Power: Issues for NATO Doctrine', 4.

Recommendation 2: NATO should learn lessons from USCYBERCOM and the Mons CyOC

Waiting to adopt a joint offensive capability in the future would give NATO time to learn both how to better conduct successful cyber-deterrence and how to overcome frictions when integrating sovereign capabilities. First, NATO should use the next few years to learn from USCYBERCOM's experience of persistent engagement. Since cyber-deterrence is such a new field, seeing what has worked in practice will help other members agree on the sorts of cyberweapons they need to develop and the scenarios in which they would use them. For instance, if persistent engagement works, consensus may grow around the need for less complex cyberweapons that can be quickly developed. Second, NATO should see the CyOC as a stepping-stone on the road to a joint offensive capability. The CyOC represents an opportunity to learn many lessons about the organisational integration of sovereign capabilities, such as where the doctrinal fault lines between allies lie and how C2 could be improved.

Recommendation 3: Create a Cyber Planning Group (CPG) with voluntary opt-in from states

A CPG would act as a forum to discuss NATO's offensive cyber policy, that would work alongside the CyOC by helping to overcome political divisions. It could be modelled on the Nuclear Planning Group (NPG), which members use to review and adapt the Alliance's nuclear policy.[247] For now, a CPG could focus on drafting standardised offensive cyber doctrine and rules of engagement that the CyOC is currently lacking. Having an opt-in system would help NATO circumvent some of the wider political divisions it faces, especially from Turkey and France. This worked

[247] Jason Healey and Leendert Van Bochoven, 'NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow', *Atlantic Council,* (2012), last accessed on (09/09/2020), https://www.files.ethz.ch/isn/183476/NATOs_Cyber_Capabilities.pdf, 6-7; NATO, 'Nuclear Planning Group (NPG)', *NATO*, (2020), last accessed on (09/09/2020), https://www.nato.int/cps/en/natolive/topics_50069.htm.

for the NPG, which has lasted since 1966 without French membership.[248] Meanwhile, it is more politically palatable to focus on coordinating existing capabilities rather than creating new ones. Nevertheless, a CPG would lay the foundations for a joint offensive cyber C2 structure further down the road.

Recommendation 4: Members should invest in developing cyber-attribution technologies

Allies should follow the US lead in this regard. In 2016, the Obama administration assigned $19 billion for cyber security, dedicated partly to long-term investment to develop science and technology for cyber-deterrence, including attribution technologies.[249] NATO should cooperate with the EU on this, which also needs to invest in technical capabilities to improve cyber-attribution.[250] Investing in this technology means members will be better placed to pool their cyber assets later on. First, improved attribution would make it easier to provide legal justification for using a joint offensive capability, encouraging political buy-in for its establishment and use. Second, by making retaliatory strikes more accurate, it would give political leaders more faith in their use at the national level. This would make it more politically acceptable for member states to combine their offensive assets at a later stage.

[248] Ibid.

[249] Burton, 'Cyber Deterrence: A Comprehensive Approach?', 12.

[250] Paul Ivan, 'Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox', *Europe in the World Programme,* 18, (2019), 11.

Conclusion

Overall, a joint offensive cyber capability would likely improve NATO's cyber-deterrence to a significant degree and would certainly improve collective defence. However, the practical and legal obstacles to a joint offensive cyber capability mean it would be unrealistic for NATO to acquire one in the next few years. Nonetheless, this thesis recommends that the Transatlantic Alliance *should* pool members' sovereign cyber assets in the long-term, taking several measures in the interim to facilitate this.

Chapter 1 gave a brief overview of NATO's history with cybersecurity and its current doctrine. It showed that since the 2007 Estonia attacks, NATO has faced ever increasing cyberattacks, principally from Russia and China. In response, it has founded defensive cyber bodies like the CCD CoE, committed to coordinating cyber-defence, established cyber as a fifth operational domain and announced that cyberattacks could trigger Article 5. Attacks have continued nevertheless, while members will likely become increasingly vulnerable as their reliance on IT systems continues. Crucially, NATO began to reverse its defensive mandate in cyberspace by announcing the CyOC in 2017, with the aim of integrating members' cyberweapons for defence and deterrence. Chapter 1 also explained what cyberweapons are and introduced the unresolved academic debate over cyber deterrence-by-denial and deterrence-by-punishment.

Chapter 2 analysed the debate in more detail, arguing that both forms of deterrence face serious challenges of credibility, meaning their respective limitations *strengthen* the need for them to complement each other. It highlighted that cyber deterrence-by-punishment is possible, despite the criticism it receives in the literature, because cyber-deterrence needs to be framed in *cumulative* rather than absolute terms. Chapter 2 gave three main reasons why a joint offensive cyber capability would enhance NATO's cyber-deterrent posture. It would: improve intra-alliance knowledge transfer of cyber-intelligence gathering and cyber-sabotage techniques; help coordinate attacks and mitigate fratricide; and accelerate decision-making and streamline response scenario planning. It emphasised that cyber deterrence-by-punishment is *not* a silver bullet, but a means of improving deterrence alongside defensive measures by changing adversaries' cost-benefit calculus. It then countered the various criticisms of cyber deterrence-by-punishment. First, it argued that attributing cyberattacks is not as hard as some scholars contend and that a joint capability would facilitate attribution. Second, signalling is not as important in cyberspace as it was for nuclear deterrence, while USCYBERCOM's posture of persistent engagement suggests that signalling in cyberspace may switch from parading to *using* capabilities. Third, pooling sovereign capabilities would likely make them less escalatory and less likely to cause collateral damage, due to centralised C2 and improved control. Fourth, it argued that acquiring such a capability would not fuel an arms race, because Russia and China already possess many cyberweapons. Finally, Chapter 2 argued that a joint capability would certainly bolster collective defence through the provision of battlefield effects. It would improve upon the CyOC, by accelerating commanders' decision-making and improving coordination with conventional assets.

Chapter 3 then argued that despite the advantages of a combined offensive cyber capability, NATO would have to overcome serious practical obstacles to set one up. First, such an endeavour would be politically sensitive, because political leaders are hesitant to use cyberweapons and because NATO is lacking in cohesion. Moreover, national intelligence agencies will be very reluctant to share information necessary to conduct effective cyberoperations. This is mainly because many allies do not share strong levels of trust, shared interests and diplomatic relations with each other. Chapter 4 built on this by outlining the legal hurdles NATO would face in establishing and using a joint cyber capability. Though there are some basic legal parameters that dictate when retaliation in cyberspace is justified, many legal uncertainties remain. In particular, it is unclear what constitutes a 'use of force' that justifies retaliation. Though there are clearer rules on how to comply with cyber *jus in bello*, it can be hard to ensure retaliatory strikes abide by the principles of distinction and proportionality. Finally, it would likely be challenging to pool members' sovereign capabilities in the first place, because they currently abide by different legal codes in cyberspace.

Taking these stumbling blocks into account, Chapter 5 acknowledged that attempting to pool members' cyberweapons would be unrealistic in the short-term. Nonetheless, it recommended that NATO seek this capability in the future, both to improve collective defence and deterrence in the face of ever increasing cyber-threats. Due to cyberweapons' imperfections and the legal constraints on their use, they need to be integrated into an FDO package with other measures to give NATO flexible response options. Furthermore, NATO members need to take measures now to prepare the ground for a joint capability. This includes: learning lessons about persistent engagement doctrine and the organisational integration of cyberweapons from USCYBERCOM and the CyOC; creating a CPG with voluntary opt-in from states; and investing in the development of cyber-attribution technologies.

Bibliography

Alatalu, Siim, 'One Year After Warsaw: The Growing Need for a NATO Cyber Command', *NATO CCDCOE*, (2017), last accessed on (09/09/2020), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8167513&casa_token=QkFD97XIVmgAAAAA:tPF8ETfDvqcdXmHmq2ON76rB8s5lJBNoqHjuEixuSfbkyjBvfCw9qzGKOMbNw4hCeQ8FYo0B

Aldrich, Richard, 'Transatlantic Intelligence and Security Cooperation', *International Affairs*, 80:4, (2004)

Ali, Rizwan, 'NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons', *Foreign Policy*, (2017), last accessed on (09/09/2020), https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/

Argote, Linda and Ingram, Paul, 'Knowledge Transfer: A Basis For Competitive Advantage In Firms', *Organizational Behavior and Human Decision Processes*, 82:1, (2000)

Art, Robert, 'To What Ends Military Power?', *International Security*, 4:4, (1980)

Arts, Sophie, 'Offense As the New Defense: New Life for NATO's Cyber Policy', *The German Marshall Fund of the United States,* 39, (2018)

Ballast, Jan, 'Trust (in) NATO: The Future of Intelligence Sharing Within the Alliance', *NATO Defence College*, (2017), last accessed on (09/09/2020), https://rieas.gr/images/rieasnews/NATOarticle17.pdf

BBC News, 'Energy Firms Hacked by 'Cyber-espionage Group Dragonfly', *BBC News*, (2014), last accessed on (09/09/2020), https://www.bbc.co.uk/news/technology-28106478

BBC News, 'How a Cyber Attack Transformed Estonia', *BBC News*, (2017), last accessed on (09/09/2020), https://www.bbc.co.uk/news/39655415#:~:text=On%2026%20April%202007%20Tallinn,in%20some%20cases%20lasted%20weeks.&text=Such%20attacks%20are%20not%20specific%20to%20tensions%20between%20the%20West%20and%20Russia

BBC News, 'US to Withdraw 12,000 Troops from Germany in 'Strategic' Move', *BBC News*, (2020), last accessed on (09/09/2020), https://www.bbc.co.uk/news/world-us-canada-53589245

Bendiek, Annegret and Metzger, Tobias, 'Deterrence Theory in the Cyber-century', *Informatik,* (2015)

Bernasconi, Claudia, 'NATO's Fight Against Terrorism: Where Do We Stand?', *NATO Defence College*, 66, (2011)

Blank, Laurie, 'International Law and Cyber Threats from Non-state Actors', *US Naval War College International Law Studies*, 89, (2013)

Brangetto, Pascal, Minárik, Tomáš and Stinissen, Jan, 'From Active Cyber Defence to Responsive Cyber Defence: A Way for States to Defend Themselves – Legal Implications', *NATO Legal Gazette,* 35, (2014)

Burton, Joe, 'Cyber Deterrence: A Comprehensive Approach?', *NATO CCDCOE*, (2018), last accessed on (09/09/2020), https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf

CCDCOE, 'Trends in International Law for Cyberspace', *CCDCOE*, (2019), last accessed on (09/09/2020), https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf

CNBC, 'US to Offer Cyberwar Capabilities to NATO Allies', *CNBC*, (2018), last accessed on (09/09/2020), https://www.cnbc.com/2018/10/03/us-to-offer-cyberwar-capabilities-to-nato-allies.html

Connell, Michael and Vogler, Sarah, 'Russia's Approach to Cyber Warfare', *Center for Naval Analyses*, (2017), last accessed on (09/09/2020), https://apps.dtic.mil/sti/pdfs/AD1032208.pdf

Crosston, Matthew, 'World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope For Cyber Deterrence', *Strategic Studies Quarterly,* 5:1, (2011)

Crowdstrike, 'Who is Fancy Bear (APT28)?', *Crowdstrike*, (2019), last accessed on (09/09/2020), https://www.crowdstrike.com/blog/who-is-fancy-bear/

Davies, Martin, 'Knowledge – Explicit, Implicit and Tacit: Philosophical Aspects', in *International Encyclopaedia of the Social & Behavioral Sciences*, ed. James Wright, (New York: Elsevier, 2015)

Davis, Susan, 'NATO In The Cyber Age: Strengthening Security & Defence, Stabilising Deterrence', *NATO Parliamentary Assembly*, (2019), last accessed on (09/09/2020), https://nato-pa.int/download-file?filename=sites/default/files/2019-

10/REPORT%20148%20STC%2019%20E%20rev.%201%20fin%20%20-%20NATO%20IN%20THE%20CYBER%20AGE.pdf

Denning, Dorothy, 'Rethinking The Cyber Domain and Deterrence', *Joint Forces Quarterly*, 77, (2015)

Dinniss, Heather, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives', *Israel Law Review*, 48:1, (2015)

Dinniss, Heather, *Cyber Warfare and the Laws of War*, (Cambridge: Cambridge University Press, 2012)

Ellehuus, Rachel, 'Turkey and NATO: A Relationship Worth Saving', *Center for Strategic and International Studies*, (2019), last accessed on (09/09/2020), https://www.csis.org/analysis/turkey-and-nato-relationship-worth-saving

EURACTIV, 'NATO Sees New Cyber Command Centre by 2023 as Europe Readies for Cyber Threats', *EURACTIV*, (2018), last accessed on (09/09/2020), https://www.euractiv.com/section/defence-and-security/news/nato-sees-new-cyber-command-centre-by-2023-as-europe-readies-for-cyber-threats/

EURACTIV, 'Turkey Not Backing Down in NATO Defence Plans Dispute – Source', *EURACTIV*, (2019), last accessed on (09/09/2020), https://www.euractiv.com/section/defence-and-security/news/turkey-not-backing-down-in-nato-defence-plans-dispute-source/

Fernholz, Tim, 'How Google is Fighting ISIL in Syria', Quartz, (2015), last accessed on (09/09/2020), https://qz.com/476882/how-google-is-fighting-isis-in-syria/

Fujii, Hideyuki, 'Deterrence by Resilience in Cyberspace', in *Cyber Defense: Policies, Operations and Capacity Building,* ed. Sandro Gaycken, (Amsterdam: IOS Press, 2019)

Gartzke, Erik and Lindsay, Jon, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', *Security Studies*, 24:2, (2015)

Gaub, Florence, 'Global Trends to 2030: Challenges and Choices for Europe', *European Strategy and Policy Analysis System,* (2019), last accessed on (09/09/2020), https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/ESPAS_Report2019.pdf

Geers, Kenneth, 'The Challenge of Cyber Attack Deterrence', *Computer Law & Security Review,* 26:3, (2010)

Greenberg, Andy, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, (2018), last accessed on (09/09/2020), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Gruszczak, Artur, ‘NATO’s Intelligence Adaptation Challenge’, *GLOBSEC,* (2018), last accessed on (09/09/2020), https://www.globsec.org/wp-content/uploads/2018/03/NATO%E2%80%99s-intelligence-adaptation-challenge.pdf

Healey, Jason and Van Bochoven, Leendert, ‘NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow’, *Atlantic Council,* (2012), last accessed on (09/09/2020), https://www.files.ethz.ch/isn/183476/NATOs_Cyber_Capabilities.pdf

Healey, Jason, ‘The Implications of Persistent (and Permanent) Engagement in Cyberspace’, *Journal of Cybersecurity,* 5:1, (2019)

Herzog, Stephen, ‘Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses’, *Journal of Strategic Security*, 4:2, (2011)

Hoffman, Wyatt and Levite, Ariel, ‘Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?’, *Carnegie Endowment for International Peace,* (2017), last accessed on (09/09/2020), https://carnegieendowment.org/files/Brief-Cyber_Defense.pdf

Hughes, Rex, ‘NATO and Cyber Defence: Mission Accomplished?’, *Atlantisch Perspectief*, 33, (2009)

Hunker, Jeffrey, ‘Cyber War and Cyber Power: Issues for NATO Doctrine’, *NATO Defence College*, 62, (2010)

Iftimie, Ion, ‘NATO’s Needed Offensive Cyber Capabilities’, *NATO Defence College Policy Brief,* (2020), last accessed on (09/09/2020), http://www.ndc.nato.int/download/downloads.php?icode=643

Inayeh, Alina, Unluhisarcikli, Ozgur and Baranowski, Michal, ‘Avoiding the East-South Divide Ahead of the NATO Summit’, *The German Marshall Fund of the United States,* (2016), last accessed on (09/09/2020), https://www.gmfus.org/blog/2016/06/08/avoiding-east-south-divide-ahead-nato-summit

Infosec, ‘SCADA & Security of Critical Infrastructures’, *Infosec,* (2020), last accessed on (09/09/2020), https://resources.infosecinstitute.com/scada-security-of-critical-infrastructures/#gref

Ivan, Paul, ‘Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox’, *Europe in the World Programme,* 18, (2019) Jinghua, Lyu, ‘What Are China’s Cyber Capabilities and Intentions?’, *Carnegie Endowment for International Peace*, (2019), last accessed on (09/09/2020), https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

Joubert, Vincent, ‘Five Years After Estonia's Cyber Attacks: Lessons Learned For NATO?’, *NATO Defence College*, 76, (2012)

Kaspersky, ‘What is a Computer Virus or a Computer Worm?’, *Kaspersky*, (2020), last accessed on (09/09/2020), https://www.kaspersky.co.uk/resource-center/threats/viruses-worms

Kello, Lucas, ‘The Meaning of the Cyber Revolution: Perils to Theory and Statecraft’, *International Security*, 38:2, (2013)

Kello, Lucas, *The Virtual Weapon and International Order*, (New Haven: Yale University Press, 2017)

Kramer, Franklin, Butler, Robert and Lotrionte, Catherine, ‘Cyber, Extended Deterrence, and NATO’, *Atlantic Council*, (2016), last accessed on (09/09/2020), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf

Kushner, David, ‘The Real Story of Stuxnet’, *IEEE Spectrum,* 3:50, (2013)

Lau, Felix, Rubin, Stuart, Smith, Michael and Trajkovic, Ljiljana, ‘Distributed Denial of Service Attacks’, *IEEE*, 3, (2000)

Lewis, James, ‘Cyberspace and Armed Forces: The Rationale for Offensive Cyber Capabilities’, *Australian Strategic Policy Institute*, (2016), last accessed on (09/09/2020), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/SI106_Cyberspace_armed-forces.pdf?8yAfEkjjYGgLpD0F3xF100AF5RHS.kPo

Lewis, James, ‘Strategy After Deterrence’, *Center for Strategic and International Studies*, (2020), last accessed on (09/09/2020), https://www.csis.org/analysis/strategy-after-deterrence

Lewis, James, ‘The Role of Offensive Cyber Operations in NATO’s Collective Defence’, *Tallinn Paper,* 9, (2015)

Libicki, Martin, ‘Cyberdeterrence and Cyberwar’, *RAND Corporation*, (2009)

Lin, Herbert and Smeets, Max, ‘Offensive Cyber Capabilities: To What Ends?’, *NATO CCDCOE*, (2018), last accessed on (09/09/2020), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8405010&casa_token=4f6mqji

YAIIAAAAA:yHTbI7EpGIGORExYG3SEFEkevH8Y6vLPVpG_gtZUqghqLnLuvJVJerKvHFM8BNn6CbQzik6H&tag=1

Lin, Herbert, 'Offensive Cyber Operations and the Use of Force', *Journal of National Security Law & Policy*, 4, (2010)

Lynn III, William, 'Defending a New Domain - The Pentagon's Cyberstrategy', *Foreign Affairs*, 89, (2010)

Mahoney, Keenan, Rovner, Joshua, Mladenovic, Nemanja, Molina, Salvador, Scher, Adam, Stern, Selma, and Zoia, Christopher, 'NATO Intelligence Sharing in the 21st Century', *Columbia School of International and Public Affairs*, (2017)

Morgan, Patrick, 'Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm', in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, (Washington, DC: National Academies Press, 2010)

Muller, Lilly, 'Military Offensive Cyber-Capabilities: Small-State Perspectives', *NUPI Policy Brief*, (2019), last accessed on (09/09/2020), https://nupi.brage.unit.no/nupi-xmlui/handle/11250/2583385

National Public Radio, 'How The U.S. Hacked ISIS', *National Public Radio,* (2019), last accessed on (09/09/2020), https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis?t=1599413589681

NATO, 'AJP-3 Allied Joint Doctrine for the Conduct of Operations', *NATO*, (2019), last accessed on (09/09/2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf

NATO, 'Cyber Defence Pledge', *NATO*, (2016), last accessed on (09/09/2020), https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO, 'Cyber Defence', *NATO*, (2020), last accessed on (09/09/2020), https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO, 'Deterrence and Defence', *NATO*, (2020), last accessed on (09/09/2020), https://www.nato.int/cps/en/natohq/topics_133127.htm

NATO, 'NATO Cyber Defence Fact Sheet', *NATO*, last accessed on (09/09/2020), https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf

NATO, 'Nuclear Planning Group (NPG)', *NATO*, (2020), last accessed on (09/09/2020), https://www.nato.int/cps/en/natolive/topics_50069.htm

NATO, 'Preparing for Tomorrow: Cyber Defence and the New Strategic Concept', *NATO*, (2011), last accessed on (09/09/2020), https://www.nato.int/cps/en/natolive/news_77515.htm

NATO, 'Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization', *NATO*, (2010), last accessed on (09/09/2020), https://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf

NATO, 'The NATO Command Structure Factsheet', *NATO*, (2018), last accessed on (09/09/2020), https://www. nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/1802-Factsheet-NATO-CommandStructure_en.pdf

NATO, 'The NATO Force Structure', *NATO*, (2015), last accessed on (09/09/2020), https://www.nato.int/cps/en/natohq/topics_69718.htm

Nomikos, John, 'A European Intelligence Service for Confronting Terrorism', *International Journal of Intelligence and CounterIntelligence*, 18:2, (2005)

Nye, Joseph, 'Deterrence and Dissuasion in Cyberspace', *International Security,* 41:3, (2017)

Ottis, Rain, 'Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective', *NATO CCDCOE*, (2008), last accessed on (09/09/2020), https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Paravicini, Giulia, 'Europe's Intelligence 'Black Hole', *Politico*, (2015), last accessed on (09/09/2020), https://www.politico.eu/article/europes-intelligence-black-hole-europol-fbi-cia-paris-counter-terrorism/

Pomerleau, Mark, 'Here Are the Problems Offensive Cyber Poses for NATO', *Fifth Domain*, (2019), last accessed on (09/09/2020), https://www.fifthdomain.com/international/2019/11/20/here-are-the-problems-offensive-cyber-poses-for-nato/

Pomerleau, Mark, 'What is 'Sovereignty' in Cyberspace? Depends Who You Ask', *Fifth Domain*, (2019), last accessed on (09/09/2020), https://www.fifthdomain.com/international/2019/11/21/what-is-sovereignty-in-cyberspace-depends-who-you-ask/

Ranger, Steve, 'NATO Updates Policy: Offers Members Article 5 Protection Against Cyber Attacks', *Atlantic Council*, (2014), last accessed on (09/09/2020), https://www.atlanticcouncil.org/blogs/natosource/nato-updates-policy-offers-members-article-5-protection-against-cyber-attacks/

Rattray, Gregory and Healey, Jason, 'Categorizing and Understanding Offensive Cyber Capabilities and Their Use', in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*, (Washington, DC: National Academies Press, 2010)

Reuters, 'NATO Cyber Command to be Fully Operational in 2023', *Reuters*, (2018), last accessed on (09/09/2020), https://uk.reuters.com/article/uk-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUKKCN1MQ1ZT

Reuters, 'Yahoo Says Hackers Stole Data From 500 Million Accounts in 2014', *Reuters*, (2016), last accessed on (09/09/2020), https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-hackers-stole-data-from-500-million-accounts-in-2014-idUSKCN11S16P#:~:text=Yahoo%20says%20hackers%20stole%20data%20from%20500%20million%20accounts%20in%202014,-Dustin%20Volz&text=(Reuters)%20%2D%20Yahoo%20Inc%20YHOO,known%20cyber%20breach%20by%20far

Rid, Thomas and Buchanan, Ben, 'Attributing Cyber Attacks', *Journal of Strategic Studies*, 38:2, (2015)

Rid, Thomas, 'Cyber War Will Not Take Place', *Journal of Strategic Studies*, 35:1, (2012)

Rosen, Nachama, 'How are Multinational NATO Operations Responsible for International Humanitarian Law Violations', *Fletcher Forum of World Affairs,* 37:3, (2013)

Russell, Alison, 'Strategic Anti-access/Area Denial in Cyberspace', *NATO CCDCOE,* (2015), last accessed on (09/09/2020), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7158475&casa_token=aYyp4LcV1B0AAAAA:0_xoO1wlkDtp6eWDedSgmUY_oyWBQSTkYmItuml272dqgnAbX5MlOcLr1IYASTcp-n1mJi52&tag=1

Schmitt, Michael, 'The Law of Cyber Targeting', *Naval War College Review*, 68:2, (2015)

Schmitt, Michael, 'The Law of Cyber Warfare: Quo Vadis', *Stanford Law and Policy Review,* 25, (2014)

Sexton, Mark, 'UK Cybersecurity Strategy and Active Cyber Defence – Issues and Risks', *Journal of Cyber Policy,* 1:2, (2016)

SHAPE, '1949-1952: Creating A Command Structure for NATO', *SHAPE*, (2020), last accessed on (09/09/2020), https://shape.nato.int/page14612223.aspx

Shea, Jamie, 'How is NATO Meeting the Challenge of Cyberspace?', *Prism*, 7:2, (2017)

Shea, Jamie, 'NATO: Stepping Up Its Game in Cyber Defence', *Cyber Security: A Peer-Reviewed Journal*, 1:2, (2017)

Sigholm, Johan, 'Non-state Actors in Cyberspace Operations', *Journal of Military Studies*, 4:1, (2013)

Smeets, Max, 'Europe Slowly Starts to Talk Openly About Offensive Cyber Operations', *Council on Foreign Relations*, (2017), last accessed on (09/09/2020), https://www.cfr.org/blog/europe-slowly-starts-talk-openly-about-offensive-cyber-operations

Smeets, Max, 'Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment', *Defence Studies*, 18:4, (2018)

Taddeo, Mariarosaria, 'The Limits of Deterrence Theory in Cyberspace', *Philosophy & Technology*, 31:3, (2018)

The Economist, 'Emmanuel Macron Warns Europe: NATO is Becoming Brain-dead', *The Economist*, (2019), last accessed on (09/09/2020), https://www.economist.com/europe/2019/11/07/emmanuel-macron-warns-europe-nato-is-becoming-brain-dead

The Economist, 'NATO Members' Promise of Spending 2% of Their GDP on Defence is Proving Hard to Keep', *The Economist*, (2019), last accessed on (09/09/2020), https://www.economist.com/special-report/2019/03/14/nato-members-promise-of-spending-2-of-their-gdp-on-defence-is-proving-hard-to-keep

The Guardian, 'DDoS Attack That Disrupted Internet Was Largest of its Kind in History, Experts Say', *The Guardian*, (2016), last accessed on (09/09/2020), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

The Guardian, 'UK To Launch Specialist Cyber Force Able To Target Terror Groups', *The Guardian*, (2020), last accessed on (09/09/2020), https://www.theguardian.com/technology/2020/feb/27/uk-to-launch-specialist-cyber-force-able-to-target-terror-groups

The National Interest, 'Hacked: How China Stole U.S. Technology for Its J-20 Stealth Fighter', *The National Interest,* (2019), last accessed on (09/09/2020), https://nationalinterest.org/blog/buzz/hacked-how-china-stole-us-technology-its-j-20-stealth-fighter-66231

The New York Times, ‘Obama Order Sped Up Wave of Cyberattacks Against Iran’, *The New York Times*, (2012), last accessed on (09/09/2020), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

The Washington Post, ‘Russian Military was Behind ‘NotPetya’ Cyberattack in Ukraine, CIA Concludes’, *The Washington Post*, (2018), last accessed on (09/09/2020), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

The Washington Post, ‘U.S., Israel Developed Flame Computer Virus To Slow Iranian Nuclear Efforts, Officials Say’, *The Washington Post*, (2012), last accessed on (09/09/2020), https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

The Washington Post, ‘White House Authorizes ‘Offensive Cyber Operations’ to Deter Foreign Adversaries’, *The Washington Post*, (2018), last accessed on (09/09/2020), https://www. washingtonpost.com/world/national-security/trump-authorizes-offensive-cyberoperations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8- b7d2-0773aa1e33da_story.html?utm_term=.1f668d182794

Thornton, Rod and Miron, Marina, ‘Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom’, *Journal of Cyber Policy*, 4:2, (2019)

Tolga, İhsan Burak, ‘Principles of Cyber Deterrence and the Challenges in Developing a Credible Cyber Deterrence Posture’, *NATO CCDCOE*, (2018), last accessed on (09/09/2020), https://pdfs.semanticscholar.org/9549/e0fc5b5e87fad6979d9d910eb10e25dbdeab.pdf

Tor, Uri, ‘Cumulative Deterrence’ As A New Paradigm For Cyber Deterrence’, *Journal of Strategic Studies*, 40:2, (2017)

Trujillo, Clorinda, ‘The Limits of Cyberspace Deterrence’, *Joint Forces Quarterly*, 75, (2014)

Tucker, Patrick, ‘How NATO Is Preparing to Fight Tomorrow’s Cyber Wars’, *Defense One*, (2017), last accessed on (09/09/2020), https://www.defenseone.com/technology/2017/10/how-nato-preparing-fight-tomorrows-information-wars/142084/

Unal, Beyza, 'Cybersecurity of NATO's Space-based Strategic Assets', *Chatham House*, (2019), last accessed on (09/09/2020), https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf

United Kingdom, 'National Cyber Security Strategy, 2016 – 2021', (2016), last accessed on (09/09/2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

United Kingdom, Intelligence and Security Committee of Parliament, 'Russia Report', (2020), last accessed on (09/09/2020), https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl

USCYBERCOM, 'Achieve and Maintain Cyberspace Superiority', *USCYBERCOM*, (2018), last accessed on (09/09/2020), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

Veenendaal, Matthijs, Kaska, Kadri and Brangetto, Pascal, 'Is NATO Ready To Cross The Rubicon On Cyber Defence?', *NATO CCDCOE,* (2016), last accessed on (09/09/2020), https://www.ccdcoe.org/uploads/2018/10/NATO-CCD-COE-policy-paper.pdf

von Loringhoven, Arndt Freytag, 'A New Era for NATO Intelligence', *NATO Review*, (2019), last accessed on (09/09/2020), https://www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html

Walsh, James, *The International Politics of Intelligence Sharing*, (New York: Columbia University Press, 2009)

War on The Rocks, 'A Close Look At France's New Military Cyber Strategy', *War on The Rocks,* (2019), last accessed on (09/09/2020), https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/

Wright, Jeremy, 'Cyber and International Law in the 21st Century', *UK Government*, (2018), last accessed on (09/09/2020), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century