NATO PARLIAMENTARY ASSEMBLY
ASSEMBLEE PARLEMENTAIRE DE L'OTAN

DEFENCE AND SECURITY COMMITTEE (DSC)
SUB-COMMITTEE ON FUTURE SECURITY AND DEFENCE CAPABILITIES (DSCFC)

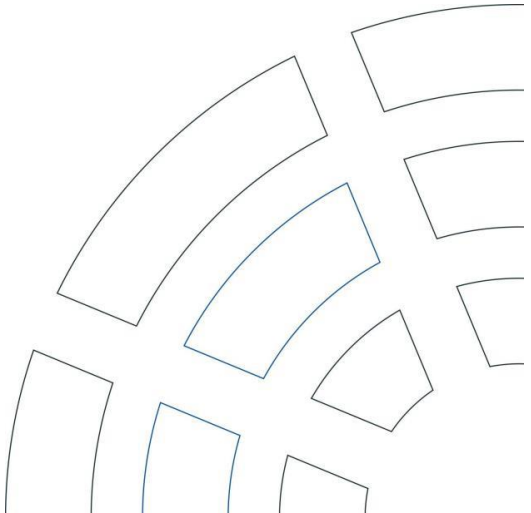
DRAFT REPORT

THE OFFENCE-DEFENCE BALANCE: NATO'S GROWING CYBER CHALLENGE

Draft Report
Roberta PINOTTI (Italy)
Rapporteur

015 DSCFC 22 E rev.1 – Original: English – 22 September 2022

Founded in 1955, the NATO Parliamentary Assembly acts as a consultative interparliamentary organisation which is institutionally separate from NATO. This working document only represents the views of the Rapporteur until it has been adopted by the Committee. It is based on information from publicly available sources or NATO PA meetings – which are all unclassified.



EXECUTIVE SUMMARY

The rise of cyber operations - both below and above the threshold of war - raises significant questions about the future of Allied security, and of warfare more broadly. As NATO's new Strategic Concept states: "Cyberspace is contested at all times." The cyber challenge facing Allies today, the Strategic Concept notes, is one wherein – 'Malign actors seek to degrade our critical infrastructure, interfere with our government services, extract intelligence, steal intellectual property and impede our military activities." Economic disruption and civil society fracturing could be added to this – as the scope of the challenge is only growing with digital network dependence, which, in the parlance of cyber experts, means Allies are faced with an increasingly vast 'threat surface'.

As a result, defending critical infrastructure, financial markets, and even social stability from cyberattacks has not only become increasingly difficult, but also increasingly vital. In addition to government and private sector investment in knowhow and capabilities to protect their networks, militaries around the world need to revise their doctrines, as they integrate new types of operations into their capabilities and learn to digitally attack and defend ever "smarter" materiel, weapons, and command and control structures.

This revised draft report outlines current technical concepts, threat actors, and key areas of focus of the debate on cyber conflict. It seeks to guide the transatlantic parliamentary discussion around these issues at a time where NATO is increasingly focused on cyberspace challenges; in recent years, the Alliance adopted a Comprehensive Cyber Defence Policy, and reaffirmed the validity of the Atlantic Treaty's Article 5 in cyberspace – cyber also featured prominently on the agenda at the Madrid 2022 Summit and is a strong focus of its outcomes.

This report first establishes definitional clarity for the logics underpinning cyber effects. It then explores the growing impact of cyber attacks on warfare, catalysed by emerging technologies, posing numerous challenges in the operational and legal realms. It then goes over the cyber doctrines and capabilities of NATO's two principal cyberspace challengers, China and Russia. It subsequently provides an overview of NATO's current and evolving policies on cyber defence. Finally, it sums up some early insights from the cyber effects seen in the ongoing Russian-Ukrainian war and the key cyber outcomes of the Madrid Summit.

Due to the nature of technological development, cyberspace is certain to become an even more contested domain. To this end, NATO Parliamentarians should collaborate to ensure continued and increased investment in the interoperability of Allied cyber forces. They should ensure that threats as broad as cyber attacks are well understood and defended against not only by militaries and governments, but also by the private sector and civil society through enhanced dialogue and cooperation. As the report concludes, building resilient transatlantic cyber defences requires finding common ground on legal frameworks regarding cyberspace; attributing and dealing with cyber incidents as an Alliance; and working with partners capable of enhancing collective cyber defences or requiring acute support - like Ukraine.

TABLE OF CONTENTS

I- INTRODUCTION

1. At all levels – from the local to the global – human society is increasingly wired into an interdependent and growing digital web. This vast scale of interconnectedness has reaped benefits in terms of prosperity and productivity, but it has also exposed societies to profound risks. A well-executed cyber operation has an increasing potential to damage and destroy critical infrastructure, disrupt financial markets, and even undermine political and social stability.

2. Modern militaries are increasingly dependent on digital support systems. Today's armed forces' platforms require sophisticated software and interdependent cyber networks for battlefield manoeuvre, understanding, and mission execution. As dependence on these cyber systems seeps into every aspect of military organisation, the vulnerabilities of modern military systems to cyber operations grow. Efforts to exploit the potential weaknesses in these modern systems have given rise to sophisticated cyber warfare effects across a growing number of nations, as well as the electronic warfare means to thwart them.

3. Recognising these vulnerabilities, NATO continues to work to hone the cyber capabilities and, therefore, defences of all Allies and partners. Allies' 2021 Comprehensive Cyber Defence Policy works to support NATO's three core tasks – collective defence, crisis management, and cooperative security – and broader defence and deterrence posture, as well as enhance resilience. At the June 2022 Madrid Summit, Allies committed to 'build and exercise a virtual rapid response cyber capability' in response to the growing efforts of malign actors to disrupt and degrade Allies via cyberattacks. The newly adopted Strategic Concept also notes a commitment to an expedited digital transformation of the NATO Command Structure in large part to 'enhance cyber defences, networks, and infrastructure," which is seen as an essential to maintaining "effective defence and deterrence." Allies' cooperative cyber security outreach has been on display during Russia's unprovoked invasion of Ukraine – Ukraine's cyber defences have performed beyond most experts' expectations, thwarting major cyber operations against critical government, military, and civilian infrastructure, and mitigating the impact of those attacks that made it through.

4. This revised draft report can serve as an overview of the topic with recommendations for Parliamentarians as they weigh the growing complexity of the cyber challenge to both their own nations' interests, as well as those of the broader Alliance and its extensive partner network. It works to highlight the ability of modern cyber operations to deceive, degrade, deny, disrupt, destroy the increasingly vital and interconnected cyber assets upon which our societies depend. As it makes clear, in a domain in which the offence has the advantage, Allies must redouble their focus on endowing themselves with the capabilities to deter, defend against, and counter cyber threats.

II- CYBER CONFLICT: DEFINITIONAL CLARITY AND THREAT ACTORS

5. Concepts pertaining to "cyberspace", e.g., security or conflicts in cyberspace, are relatively novel and are often misused or poorly understood in policy discourse (Veale & Brown, 2021). One key challenge is they describe a complex and constantly fluctuating environment. Another is that divisive geopolitics preclude common understandings of what constitutes cybersecurity and cyber norms of behaviour. (ICC, 2021) Still, the following serve as accurate and parsimonious definitions for the purposes of this report.

6. ***Cyberspace*** is "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the

Internet, telecommunications networks, computer systems, and embedded processors and controllers." (US DOD, 2018) A ***cyber attack*** will aim to deceive, degrade, deny, disrupt, destroy assets (both virtual and physical), while ***cybersecurity*** is "the art of protecting networks, devices, and data from unauthorised access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information." (CISA, 2019)

7. The identity, motives, means, and level of sophistication of cyber threat actors vary significantly, and their potential targets cover a broad range; from government and military to the private sector, as well as civilian actors and critical infrastructures – essentially, anything that can run code or be connected to a network. A simplified representation (see annex 1) characterises common threat actor types and their motivations – Still, these can vary, intertwine, or even be used as proxies (knowingly or unknowingly) hiding other intentions.

8. The most sophisticated threat actors are commonly referred to as Advanced Persistent Threat groups (APTs). Only nation-states (military or intelligence) or, rarely, well-organised criminal groups qualify as APTs, as they require significant organisation and funding. Due to their stealth capabilities, a major challenge when facing APTs is not only the damage they can cause, but also correct attribution (CCCS, 2020). With sufficient successful obfuscation, one threat actor can disguise itself as another in a false-flag attack. A notable example is the Turla/OilRig case, in which a Russian state-sponsored hacker group (Turla) infiltrated an Iranian hacker group (OilRig). Unbeknownst to the Iranian group, the Russian hackers launched cyberattacks from the Iranian infrastructure (UK NCSC, 2019). Individual cybercriminals, hacktivists or thrill seekers usually pose less of a challenge. Their sheer numbers and the intentional or unintentional effects of their cyber activities, however, can also pose significant national security threats (CCCS, 2020).

9. The tools and methods each attacker may employ vary immensely, and attacks can target specific assets or spread widely and indiscriminately.[1] Threat actors can choose to exploit technical vulnerabilities, install malware[2] or target and exploit individuals[3]. The range of available entry points for an attack is referred to as the cyber threat surface. With the increasing digitisation of society, this surface is growing exponentially. A proliferation of computers, sensors, industrial control systems, the rise of the Internet of Things (i.e., connected devices, like refrigerators, watches, or GPS navigators) and the varying degrees of human involvement across the potential entry points contribute to complexifying cyber defence (CCCS, 2020).

III- THE GROWING IMPACT OF CYBER OPERATIONS ON WARFARE

A. CYBER CONFLICT AS A REVOLUTION IN MILITARY AFFAIRS

10. The importance of cyberspace in military affairs has been increasing steadily since the end of the 20th century. The role of networked components in weaponry and C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) has been essential to

---

1 The following source contains a cyber threat toolbox with useful definitions of the most common and relevant cyber operation methods: "Canadian Centre for Cyber Security. 'An Introduction to the Cyber Threat Environment'. Canadian Centre for Cyber Security, 2020. https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment."

2 Short for 'malicious software', malware is file or code delivered over a network to infect, steal, or conduct any other behaviour directed by the attacker.

3 This is an approach called social engineering, which can happen, for example via phishing.

this development. Advances in sensors, radars, radio communications and precision-guided munitions during the Cold War allowed for significant system-led advances in battlefield information management via increased ISR capabilities, which in turn allowed for the more effective use of precision firepower and manoeuvre – termed net-centric warfare, the information systems' networked advantages, however, also present exploitable (hackable) fault lines (Stiennon, 2015). Network-centric warfare thus gave birth to electronic warfare – a struggle between attempts to jam and spoof materiel and attempts to counter those effects. The United States' performance during the Gulf War was a clear demonstration of the strategic shift presented by net-centric warfare. In turn, both Russia and China understood the existential nature of the failure to adapt their militaries to this revolution in military affairs.

11. The turn of the century marked the beginning of early covert cyber operations – mostly focusing on espionage – such as a 1998 Russian exfiltration of data from the Pentagon, dubbed "Moonlight Maze" (Guerrero-Saade et al., 2017). At the same time, global connectivity increased at a breakneck pace: Spoofing, hacking and exfiltrating data was no longer just between militaries, but across every sector of society. Network vulnerability now threatened all sectors of society.

12. NATO had a first major reckoning with this new reality in 2007, when a politically motivated cyber operation targeted Estonia amidst a disagreement with Russia. A flurry of Denial-of-Service attacks took down Estonian governmental websites, including the parliament and various ministries, and expanded out to banks and newspapers (Connell & Vogler, 2017).[4] Even though the Russian government denied involvement, it used inflammatory rhetoric and refused to cooperate with Estonia regarding these attacks (Aday et al., 2019) Similar disruptive events were seen during the 2008 Russo-Georgia War, potentially marking the first time cyber means were used in combination with conventional military force. The Georgian government accused Russia directly, whereas the Russian government alluded to the possibility that Russian individuals might have started attacks on their own (Connell & Vogler, 2017). Finally, the 2010 Stuxnet attack on Iran also constituted a landmark event, as it was the first cyber attack to result in the physical destruction of an asset – approximately a fifth of the Natanz nuclear facility's centrifuges (Sanger, 2012).

13. These events explain the subsequent proliferation of military structures specifically dedicated to cyber operations – both in offence and defence – around the world. The attack on Estonia prompted Allies to conduct a thorough review of their cyber vulnerabilities and defences. A key outcome was the Alliance's first cyber defence policy in January 2008, and the inauguration of the NATO-accredited Cooperative Cyber Defence Centre of Excellence (CCDCOE) four months later (NATO, 2022).[5] The United States Cyber Command was launched in 2010. All Allies have since established some form of independent cyber command or branch within their armed services. An Italian cyber command, modelled on US Cyber Command, was outlined in Italy's 2015 White Paper and established in September 2017.

---

4 Russia was apparently piqued by the Estonian Government's decision to move a bronze statue of a Soviet soldier in memory of the USSR's efforts in WWII.

5 The CCDCOE also guided the initiative that would become the **Tallinn Manual in the International Law Applicable to Cyber Warfare** in the wake of the attack. As well, the report has had a significant impact in the still developing field of the application of international law to the cyber realm. The manual attempts to be a norm entrepreneur for cyberspace and cyber warfare via the application of existing international law frameworks into the cyber domain. A key proposition of the manual is that states do not have sovereignty over the Internet, but rather only over components of the Internet in their territory.

B. INCREASING POTENTIAL OF CYBER ATTACKS

14. As the Stuxnet attack demonstrated, sophisticated cyber attacks have the potential not just to disrupt networks and cripple systems, but also to destroy physical assets. The increasing potential of cyber attacks, experts warn, can potentially disrupt all forms of modern weapons systems, potentially even compromising nuclear forces (MacAskill, 2018). Cyber threat can amplify nuclear risks in two major ways: either by undermining the security of nuclear materials or nuclear facility operations, or by compromising command and control systems (NTI, 2022).

15. Because of their reliance on inherently dual-use assets (networks and data), cyber operations play a major part in the rise of hybrid threats. By default, their execution blurs the line between civilian and military infrastructure, making it hard to prevent the muddying of the boundaries of conflict. The merging and intertwining of state and non-state actors carrying out cyber attacks as proxies is yet another facet of this phenomenon (van der Waag-Cowling, 2021). Near-peer competitors such as Russia and China increasingly rely on such cyber "mercenaries" to maintain deniability for their operations (Egloff, 2022).

16. All those factors point toward the potential of cyber attacks to change contemporary warfare in quite significant ways, as they already are doing today. The role of military cyber operations in peacetime is recent and thus in still flux (Bigelow, 2019). And major changes induced by cyber operations regarding high-intensity warfare might not even be yet fathomable, as we currently "operate in a fog of peace" (Stacey, 2020).

C. A STEALTHY AND DISRUPTIVE TOOLKIT: THE CYBER OFFENCE

17. Cyber "weapons" are not weaponry in a traditional sense and are thus difficult to define - To date, no commonly agreed upon legal definition exists. Alone, they contain no destructive power, as they always need some form of network or system to latch onto, and they are, at least for now, not particularly deadly (Stevens, 2017).

18. Cyber "weapons" are incredibly varied. They range from "generic but low-potential tools to specific but high-potential weaponry", as they are "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings" – thus any usage of code that is both intentional and harmful.[6] (Rid & McBurney, 2012)

19. If not for its deadliness, what then makes a cyber offensive capability so compelling for military operations? The answer lies in its unique qualities that are unlike most military toolsets. First, cyber attacks excel at incapacitating an enemy (Buchanan et al., 2017). Operation Orchard, for instance, a 2007 Israeli airstrike on Syria managed to bypass the country's rather developed air defence system by infiltrating it and removing the radar signature of the incoming F-15 bombers and their escort, thus deceiving duty guards (Florant, 2021; Buchanan et al., 2017). Second, if correctly engineered, they minimise collateral damage, as they can be precisely targeted (Buchanan et al., 2017; Acton, 2017). The Stuxnet case is a hallmark example here, as the payload was engineered to affect the Iranian nuclear centrifuges by changing very specific parameters in the exact industrial control system model the Iranians were using. Even though the Stuxnet worm ended up spreading beyond Iran, its inner workings were uniquely tailored to the Natanz plant and did not affect other systems (Kushner, 2013). This is not a given however – some

[6] The chart in Annex 2 breaks down the different components of cyber weaponry.

attacks rely on spreading the payload as widely as possible, like ransomware attacks. Others could be too badly engineered to remain contained. Third, cyber attacks can potentially be reversed, which gives them increased flexibility compared to traditional weapons (Buchanan et al., 2017). Ransomware, for instance, enables the attacker to mount pressure on an opponent, while safeguarding the data should it need to be released. Fourth, cyber attacks are cheaper than conventional warfare, making them a useful weapon for smaller countries or non-state actors (Swinhoe, 2020).

20. Yet, mounting a cyber offensive also comes with significant drawbacks and challenges. At the tactical level, cyber operations, especially against sophisticated threats like state-actors, require tremendous preparation – Infiltrating the adversary's network, finding out which systems the networked assets run on, adapting malware to the target, or even researching yet undiscovered vulnerabilities to compromise software (so-called zero-day exploits) can take weeks, months, if not years (Acton, 2017). As such, cyber operations are not purely technical, but also involve significant initial ISR efforts (Boeke & Broeders, 2018). Second, cyber weapons are perishable goods. It is impossible to know when vulnerabilities needed to perform an attack might get patched or when an adversary might change their digital infrastructure. Thus, cyber operations require continuous efforts, as they compare to aiming at a moving target (Acton, 2017).

21. At the strategic level, cyber operations pose the added challenges of creating new and "unnecessary vulnerabilities" (Slayton, 2017). For example, the possible interpenetration of the United States' and Russia's energy grids by their respective cyber actors could open an entirely new threat surface regarding energy security (Sanger & Perlroth, 2019; Greenberg, 2021).

22. The cyber offence, whether it is used on its own ("independent, kinetic cyber effect", such as Stuxnet), as an "enabling effect" (such as the aforementioned Operation Orchard), as a "tactical-level integrated cyber effect" (for instance a fighter jet jamming an opponent's radar) or as a "persistent annoyance" (such as the Allied Coalition's persistent disruption of ISIS communication systems) signals a move away from "attrition-centric" warfare, becoming less kinetic in favour of more "dislocation and disruption" (Jacobsen, 2021; van der Waag-Cowling, 2021).

23. Emerging and disruptive technologies will further accelerate this evolution. Cyber weaponry will benefit from new technologies such as Artificial Intelligence earlier than physical platforms, as their digital nature makes implementation easier, cheaper and less prone to institutional resistance (as it would not replace a fighter pilot's role like an unmanned aerial vehicle would do for instance) (IISS, 2021). Malware is already being trained with AI to evade defences and even shapeshift while deployed, adapting its code to the systems it infects "autonomously and at machine speed", through so-called polymorphic attacks (IISS, 2021). These evolutions are nearing effective deployment speedily: "In 2018, IBM revealed a proof- of-concept tool called 'Deep Locker', which it described as an 'AI-powered evasive malware' that hides itself in other applications until it is 'unlocked' based on several triggers that could include facial recognition, geolocation, and voice recognition. Because of its use of a 'deep neural network AI model', the 'trigger condition' unlocking the attack is 'almost impossible to reverse engineer'" (IISS, 2021). With commercial availability of such technologies, the entry barrier to such advanced capabilities will also gradually be lowered, making ample room for more instability (DeSombre, 2021).

D. PLUGGING VULNERABILITIES: THE CYBER DEFENCE

24. As Joseph Nye noted in 2010: "Because the internet was designed for ease of use rather than security, the offense currently has the advantage over the defense (Nye, 2010)." This remains the case today. Compared with conventional forces, the elements needed to mount a cyber attack are comparatively fewer and less resource-intensive. As with all military operations, the attacker has the initiative in cyberspace, but cyber defence is made more complicated than in the physical

realm by the ever-expanding cyber threat surface that requires defending. Further, the increasingly vital nature of the dependence on complex cyber systems for military and economic activities – plus a suite of other social activities and communications – creates a growing number of costly vulnerabilities (Nye, 2010). Contrariwise, cyber code remains short and relatively simple and needs to find just one node of vulnerability to penetrate and move around inside a system (Friedman and Singer, 2013).

25. This does not mean, however, that defence is powerless. Defenders can set up complicated 'kill chains' to block an attack at various stages, from reconnaissance to penetration to extraction (Arquilla, 2021). Like other forms of defence in the conventional domains, cyber defence can be divided into two essential categories, *active* and *passive*. Active cyber defence efforts act against specific threats, while passive cyber defences are the efforts to protect cyber assets and systems from possible threats. For example, data encryption ensures information is essentially inaccessible to an adversary, if intercepted. Encrypting data, however, does not take the more active step of trying to prevent its interception. Anti-malware tools, however, detect malicious software and then block the code from entering the protected system (Arquilla, 2021; Denning and Strawser, 2017).

26. The military domain is particularly networked. Today's modern weapons platforms all run complex software programmes to function. The US Navy, for example, is the largest software provider in the world – developing and implementing increasingly complex ships require unprecedented amounts of software systems to run almost every function on the ship – from weapons systems to radar and fire control to the most core functions such as water, fuel, oil, and power (Eaglen, 2022) For example, the US Navy's most technologically-advanced ship, the USS Zumwalt, (DDG 1000) is the world's only stealth destroyer and runs a system called the Total Ship Computing Environment, which uses software and blade servers on the ship running over 7 million lines of code (Osborn, 2017).

27. Further, as indicated above in the discussion of the advent of net-centric and electronic warfare, the web of networks informing every move and driving decision making surrounding the evolution of the battlespace from the tactical to the strategic level presents cyber vulnerabilities to defend – from radar to radio to satellite and everything between. While governments have certainly allocated increasing resources to bolster their cyber defences and work with their contracted software providers, the demand for faster, more reliable, real-time intelligence and response to threats continues to increase and often outpaces the abilities of the dedicated defence institutions and their dedicated contractors. As such, private sector actors are increasingly bridging the gap – in essence, becoming the newest partner in the cyber defences of government institutions and assets.

28. This public-private interface has been an increasingly valuable asset across governments' defence institutions as they are able to see threats more readily coming across their vast networks in real time. Private sector actors like Mandiant, Crowdstrike, and Booz Allen Hamilton, for example, play essential roles in cyber threat intelligence, as well as cyber defence infrastructure. For example, Mandiant became a prominent player in the threat intelligence arena in 2013, when it released a report directly implicating the Chinese government in a vast array of cyber espionage. Mandiant was also responsible for discovering the "SolarWinds" attack. According to several Allies attribution reports, Russia's SVR intelligence agency used malware inserted into a network management software update from the SolarWinds company. This then infected thousands of Allied government agencies and private businesses, lingering inside of sensitive defence department systems undetected for months (Sanger, Barnes, Conger, 2022). Paradoxically, the "SolarWinds" attack also represents the risks inherent in the growth of cyber threat surface and the outsourcing of network maintenance to sensitive defence-related institutions. Public-private sector cooperation has also proven essential in the shoring up of Ukrainian cyber defences against Russian cyber attacks in the current Russia-Ukraine war. This is detailed more in Section VI below.

E. THE ATTRIBUTION CHALLENGE

29. Attribution of a cyber attack is defined as the "allocation of direct or indirect responsibility for a malicious cyber operation," and typically "involves the determination of the origin or authorship of the cyber operation." (Kastelic, 2022). Attribution occurs at three distinct levels: technical and factual, legal, and political (Kastelic, 2022; Bendiek and Schulze, 2021). This obviously happens after an intelligence level determination of attribution, whose information allows a cyber attack to be traced within a wider context in which the hostile action is seen, both from a technical point of view, but also in an interdisciplinary way and from the point of view of the broader strategic objectives use of a cyber operation may seek to achieve. Though both the legal and political elements of attribution are often intertwined and run in parallel, both are also dependent upon factual and technical attribution, which are necessary first steps in any attribution process (Kastelic, 2022).

30. Technical attribution operates by identifying the perpetrators of a cyber attack through expert analysis of cybercrime traces and various investigative actions by state intelligence agencies, corporations, or other qualified entities (Kaspersky). Experts agree that the technical aspects of cyber attack attribution have improved significantly in recent years, including the deployment of high-tech tools such as machine learning to detect anomalous behaviour on computer networks (Kuerbis et al., 2022; Brumfield, 2020). Still, technical attribution activities continue to face significant challenges. The origins of cyber operations can be obfuscated by multiple technological mechanisms such as the use of botnets, spoofing and false flags, proxy networks and VPNs, and the "dynamic allocation of IP addresses (Kastelic, 2022). Thus, obtaining unequivocal proof of attack origin is still a challenge despite advances in technical attribution (Brumfield, 2020).

31. Legal attribution is usually discussed within the context of state responsibility and whether or not a nexus can be established between an individual and state authority (Kastelic, 2022). Because no well-developed treaty regime yet exists to regulate cyberspace, the applicable regime is customary international law, which requires a) proof of state practice and b) a sense of legal obligation (Eichensehr, 2020; Kastelic, 2022). This results in some degree of ambiguity in legal attribution for two primary reasons. The first is that establishing the link between an individual and state authority in the murky realm of cyberspace can be challenging. The second is that state practice is still underdeveloped (Kastelic, 2022; Egloff, 2020; Eichensehr, 2020). That said, the flipside to this is that the response of states to cyber. attacks can shape law over the medium and long term, especially if states claim to be acting out of a sense of legal obligation (Egloff, 2020). Yet, dangers also exist in misattribution, discussed in the next paragraph.

32. Political attribution can be done in two ways: privately or publicly (Kastelic, 2022; Egloff and Wenger, 2019). If a state decides to deliberately release information regarding an attack to the public, "it is unlikely that attribution made by a nation state (or even allied states) will be accepted as neutral and authoritative by another state, especially if those states are rivals or hostile" (Kuerbis et al., 2022). This in part stems from lingering challenges to presenting unequivocal evidence of both technical and legal attribution. Technically, and as mentioned above, cyber operatives can often camouflage activities. Legally, and as also mentioned above, a nexus between state authority and an individual must be established to assign state responsibility under customary international law. This makes the potential for denial and misattribution rampant within interstate cyber relations, which could lead to dangerous escalatory measures (Kastelic, 2022).

F. THE CHALLENGE OF CYBER WEAPON PROLIFERATION

33. Cyber weapons proliferate by use, something that is not true for traditional weapons. For example, within months of the Stuxnet attack its code was being exchanged online via various networks, which allowed malign actors to incorporate them into their own attacks (Singer, 2012).

There is a growing trove of reporting on nations having their own cyberweapons stolen and then redistributed via nefarious online networks (Perlroth & Sanger, 2017; Perlroth, 2021). These malicious codes have subsequently been found in cyber attacks, for example, the North Korean cyber attacks have been recorded as using either code directly or what was learned from stolen code (Perlroth & Sanger, 2017). Another challenge is the containment of knowhow cyber experts accrue while working for state cyber forces. Intelligence officers in more powerful cyber states are often the targets of espionage operations in an effort to either have a former or active cyber expert transfer knowhow via extortion or indirectly and unwittingly via new shell employment opportunities (Perlroth, 2021). These challenges will only grow in the future as more nations develop cyber weapons, leading to an accelerated cycle of leaks and proliferation.

34. These challenges are, however, driving parallel efforts to limit cyber weapon proliferation. The Wassenaar agreement is emblematic of these efforts. The Wassenaar Agreement adheres its signatories to voluntary export controls to control and limit the sales of military software and other 'intrusion' software in parallel to existing export controls on conventional weaponry. While these export controls have been challenged by some recent cases, the Wassenaar agreement is an import broad based international effort to address the growing challenge of cyber weapons proliferation.

IV- NATO'S CHALLENGERS: DOCTRINE & CAPABILITIES

A. RUSSIA

35. Russian cyber doctrine centres on the idea that cyber warfare is part of a larger, more holistic concept of "information confrontation" as outlined in multiple important Russian strategic documents (Hakala and Melnychuk, 2021). Just as cyber war can be directed in any direction, so too can information confrontation be theoretically directed in any direction, though in the Russian case, this direction tends to be the West. In the information domain, confrontation is seen by Russia as a zero-sum geopolitical contest in which adversaries seek superiority in an "information sphere" via the manipulation of information systems in favour of national interests and preferred ideas (Russia Encyclopedia; Hakala and Melnychuk, 2021). "Information sphere" in this sense is conceptually more encompassing than "cyberspace" (IISS, 2021; Hakala and Melnychuk, 2021).

36. Russian doctrine defines the *information sphere* as "a combination of information, informatisation objects, information systems and websites within the information and telecommunications network of the Internet […], communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating social relations in the sphere" (Security Council of the Russian Federation, 2016). In this arena, cyber tactics, such as malware attacks or cyber espionage, operate in a *grey zone* alongside disinformation campaigns and other forms of information manipulation (IISS, 2021, Hakala and Melnychuk, 2021).

37. Russian doctrine supports an understanding that information space dominance is a prerequisite for victory in modern war (IISS, 2021). This belief is so strong among Russian military leaders that Chief of the General Staff, Valery V. Gerasimov, has claimed the ratio of non-military to military measures in today's security environment to be 4:1 (Tashev, Purcell, and McLaughlin, 2019). Given the Russian military's focus on its military modernisation programmes, and doctrinal emphasis on the ability to dominate in a conventional confrontation, such a ratio is likely an overstatement. Still, it demonstrates the importance the Russian military places on non-military capabilities (Tashev, Purcell, and McLaughlin, 2019; IISS, 2022).

38. Information warfare tactics have become an essential element of Russia's recent military campaigns. This has been demonstrated in the 2007 attack on Estonia, the 2008 Russia-Georgia War, the range of Russian actions in Ukraine since its 2014 intervention, and redefining narratives surrounding the war in Syria. In many cases, large-scale disinformation campaigns and cyber attacks were (and continue to be) deployed alongside conventional military operations (Deibert, Rohozinski, and Crete-Nishihata 2012; White, 2018; Markoff, 2008; Snegovaya, 2015; ISSP, 2021; Alami, 2018).[7] To varying degrees, these campaigns continue today, as Russia seeks to keep its adversaries destabilised with perpetual confrontation in the information sphere (Vermes, 2021). This latter point reflects a more general one in which Russia portrays the information sphere as an operative space of constant struggle, especially against the West or, what is seen in Russian eyes, as Western-backed movements near its borders (IISS, 2021). Indeed, Russia portrays itself as under constant information attack, which it can then use to justify its own hybrid tactics (IISS, 2021).

39. Russia possesses significant offensive cyber capabilities and has a history of engaging in attacks. Experts believe Russia's cyber capabilities have been growing in sophistication and complexity in recent years, relying more on customised malware and third-party intermediaries to reach targets (Wolff, 2021).[8] The 2017 NotPetya attacks in Ukraine, attributed to Russia by several Allies, which wiped data from the computers of banks, energy firms, and senior government officials, are a good example of this, as are the recent SolarWinds breaches targeting US government agencies (Nakashima, 2018; IISS, 2021; Wolff, 2021; Jibilian and Canales, 2021). Many attacks such as these have caused substantial harm, "including massive financial losses, interruptions to the operation of infrastructure, and disruptions to crucial software supply chains" (Wolff, 2021).

40. In the past, offensive operations have fallen under the purview of four primary actors: the Main Directorate of the General Staff (GRU/GU), the Civilian Foreign Intelligence Service (SVR), the Federal Security Service (FSB), and "patriotic hackers" and cyber criminals. The first two operate at the explicit instruction of Russian President Vladimir Putin (IISS, 2021). The GRU/GU is located within the Russian Ministry of Defence and is the main proponent of Russian cyber operations (ISSP, 2021). It was the main coordinating institution of the 2016 hack on the US Democratic National Committee and deployed the NotPetya malware against Ukraine in 2017 (IISS, 2021).

41. Of the four actors mentioned, the GRU brings with it the most brazen culture of aggression and operates with a high tolerance for risk (Wolff, 2021). The SVR is a civilian foreign intelligence service with a "growing emphasis on long-term, covert cyber espionage operations" (Wolff, 2021). This agency is generally held responsible for the aforementioned SolarWinds breach on US government systems—notable in that the breach went undetected for at least nine months (Wolff, 2021). Experts say this was in part due to "uncharacteristic restraint" in targeting a small subset of compromised victims. SVR's emphasis is on collecting intelligence rather than causing damage, and in its operations, it seeks to remain undetected (Bowen, 2021). Russia's so-called "patriotic hackers" blur the lines between state and non-state actors, as it is unclear at whose direction they operate. However, it is often noted that their operations seem to have no purpose other than to advance Russian state interests, so experts suspect they do often cooperate with the

---

7 This includes the recent use of electronic warfare technologies in Syria, which have disrupted both unmanned aerial vehicle attacks and cruise missile launches (McDermott, 2021).

8 In the past, Russia has heavily relied on purchasing malware from the black market for its attacks. Developing customised capabilities allows Russian cyber activities to greater evade existing defences (Wolff, 2021).

Russian government (IISS, 2021). A benefit of employing such hackers (as well as cyber criminals) is that they allow the Russian government to maintain plausible deniability while advancing state interests (Hakala and Melnychuk, 2021). Lastly, Russian cyber criminals perpetrate attacks outside of Russia's borders. As with "patriotic hackers," experts are uncertain how closely cyber criminals coordinate with the Russian government, but it is known some coordination exists (IISS, 2021). This outsourcing allows the Russian government to save on additional resource allocation to cyber operations (Bowen, 2021).

42. Defensive operations have been historically delegated to the FSB, which is tasked with protecting against attacks on government systems and critical national infrastructure (Bowen, 2021; IISS, 2021). Through a range of legal and regulatory changes, this agency now operates a large domestic surveillance regime in pursuit of this mission (IISS, 2021). In addition to FSB operations, some defensive operations have recently been delegated to the Ministry of Defence, such as technical defence of sensitive information and guarding against the export of sensitive technologies (IISS, 2021). Development of a "sovereign internet" is also of great important to Russian defensive cyber doctrine, as it allows further domestic control (IISS, 2021). Experts say that all these measures have a clear and explicit purpose: the operations allow the Russian government to have a "flexible, if complex, national cyber-defence system that might give Russia an advantage in a cyber conflict with another major power" (IISS, 2021). Thus, this capability functions as a classic case of deterrence-by-denial.

B. CHINA

43. China's cyber strategy has been predominantly driven by its perception of the ideological, economic, and military threat emanating from the United States—both the threat of US promotion of liberal democratic values and hard US cyber capabilities (IISS, 2021). Its main objective is to shield domestic audiences from Western influences via the Internet (Ying, 2012). To this end, China has consistently advocated for almost two decades the concept of "cyber sovereignty," whereby a country might control the portion of the Internet being used within its geographical borders (Segal, 2021; Kolton, 2017). Importantly, as one expert notes, "any successful defense of a free and open internet will require not only confronting China but also re-engaging international organizations and broader consensus across liberal democracies about online free speech and privacy" (Segal, 2021). Thus, it can be safely assumed that China views a free and open Internet as a direct threat.

44. While early Chinese cyberspace efforts aimed mainly at censorship, China realised during the last decade that due to the rise in digital espionage, it should bolster its relatively weak defensive cyber capabilities (IISS, 2021). Thus, protecting networks became an important aim of the Chinese Communist Party, as did the development of greater overall cyber power (IISS, 2021). Chinese President Xi Jinping began this process by reconfiguring and personally overseeing Chinese cyber policy, including China's first Cyberspace Security Strategy, published in 2016 (Jong-Chen, 2017; IISS, 2021). This strategy set out a range of important core tasks, most having a heavy emphasis on protecting Chinese sovereignty and improving cyber defence (Jong-Chen, 2017; IISS, 2021).

45. In addition to industrial policy for domestic production of core internet technologies, a key pillar of China's cyber strategy has been the utilisation of cyber operations beyond its own border (IISS, 2021). These have included massive espionage operations intended to acquire intellectual property and personal data, as well as disruptive operations, such as influencing Taiwanese elections, meant to exist below escalatory thresholds (IISS, 2021).

46. Like the Russians, China views offensive cyber operations as both a necessary component of modern warfare, as well as a part of a larger attempt to gain "information dominance" in support

of strategic goals (Cheng, 2013; IISS, 2021). This dominance is primarily achieved through control of the "production and flow of information" during confrontation (IISS, 2021). Importantly, Chinese military doctrine encourages pre-emption in the information space, encouraging a first-strike policy (China Aerospace Studies Institute, 2013). This position has strengthened under President Xi's leadership, with more recent People's Liberation Army (PLA) sources claiming efforts to achieve dominance in this sphere could lead to the extensive use of Artificial Intelligence in military operations, intelligence collection and decision making (IISS, 2021).

47. China has developed significant peacetime capabilities, including "influence-and-information" operations (Kurlantzick, 2018; IISS, 2021). Much like Russia's doctrine of "information confrontation," these techniques are meant to exist somewhere below escalatory thresholds. China also likely possesses offensive cyber tools for use in combat and military operations although it has not published anything relating to a cyber warfare doctrine (Kurlantzick, 2018; IISS, 2021). Other PLA documents authoritatively recognise an offensive capability, including reference to reconnaissance and attack capabilities (Chang, 2014; IISS, 2021)

48. Reconnaissance operations monitor and identify weaknesses in the computer networks of other states during peacetime so that the groundwork for confrontation is more easily laid when a conflict erupts (IISS, 2021). Chinese views are that network strikes (the way of which is paved through earlier reconnaissance) could follow very soon after the outbreak of conflict, targeting both civilian and military infrastructure (McReynolds 2015). Additionally, China is currently considering more advanced capabilities such as "integrated network electronic warfare," which would allow China to deploy "malicious algorithms into an adversary network even if a wire connection does not exist" (IISS, 2021).

49. Though Chinese offensive cyber war capabilities remain untested, the PLA and Chinese intelligence agencies have penetrated US government and commercial networks, using malware to steal sensitive information and intellectual property (Segal and Laskai, 2018; IISS, 2021; CSIS). It is assumed that during a conflict, the PLA's offensive capabilities could be used in similar ways to bring down or damage the critical systems of its adversaries (IISS, 2021).

50. Like Russia, Chinese cyber defence has mostly been pursued through strict internal regulation and massive domestic surveillance (Austin, 2018; IISS, 2021). Despite a heavy emphasis on defence since 2014, recent evidence suggests that Chinese networks are still regularly penetrated by external attacks. For example, the China Internet Network Information Center has noted that despite advances in some areas of cyber defence, the country's overall defence has actually worsened (IISS, 2021; Austin, 2018). China appears to still be in early phases of correcting for these vulnerabilities (IISS, 2021; Sacks and O'Brien, 2016).

51. Lastly, most of the PLA's capabilities are located within the Strategic Support Force (SSF) (IISS, 2021). The SSF consists of two primary pillars. These are the Space Systems Department (responsible for all space operations) and the Network System Department (responsible for strategic information operations) (IISS, 2021). The SSF is a recent conglomeration of the military's various cyber units and reports directly to China's top military decision-making body, the Central Military Commission (IISS, 2021). This more unified force is seen by experts as both able to launch complex actions involving all elements of cyberspace and to coordinate cyber, electronic, and space warfare units in a fast-moving military confrontation (IISS, 2021)

C. OTHER CHALLENGERS: THE ASYMMETRICAL POWER OF SMALL STATES IN CYBER SPACE

52. Other smaller state actors, such as Iran and North Korea, pose both direct and indirect threat to NATO member states' interests due to their cyber capabilities. For example, in 2017, North Korean operatives launched the WannaCry ransomware attack which, when finally brought under control, had managed to rip through 150 countries wreaking chaos in its wake, paralysing a vast array of networks, among them the United Kingdom's National Health Service. More recently, Albania was hit with a powerful cyber attack on 15 July 2022 that Prime Minister Edi Rama said, "threatened to paralyse public services, erase digital systems and hack into state records, steal government intranet electronic communications, and stir chaos and insecurity in the country" (Reuters, 2022). The United States and other Allies, after weeks of investigation, determined the Government of Iran to be responsible for the attack (White House, 2022; NATO, 2002(c)). As a result of the attack, the Albanian government severed all diplomatic ties with the Islamic Republic of Iran on 7 September, which cyber experts note is the strongest public response to date taken by a state to a cyber attack (Reuters, 2022). The United States and its NATO Allies rushed advanced cyber teams to assist Albania with the recovery and investigation of the incident. In a North Atlantic Council Statement, Allies note they will "continue raising [their] guard against such malicious cyber activities in the future, and support each other to deter, defend against and counter the full spectrum of cyber threats, including by considering possible collective responses" (NATO(d), 2022).

53. In addition to these states, there is also the growing potential challenge of non-state armed groups and criminal hacker groups. These groups could pose a direct challenge with a cyber terrorist operation; as their capabilities grow, they also pose a threat as they could be used as proxies by both Russia and China in their broader competition with Allies. A recent attack on Montenegro in August represents such a possibility. Hackers struck websites and databases across the country with the 'Cuba' ransomware and virus 'Zero Date'. Initial assessments believe a criminal group, potentially with Russian backing, is responsible for the attack (Savic, 2022). Again, NATO Allies and their EU partners have been working to assist Montenegro with recovery and the investigation.

54. As is clear from the above, the cyber domain presents potentially asymmetrical power possibilities to smaller states and non-state actors. Some experts have even noted that despite states' ability to aggregate more resources and hone more sophisticated methods, the smaller threat surface of a smaller state or group can outsize their potential cyber power. Further, small states may seek to support criminal hacker groups as proxy cyber forces to achieve their ends, while holding on to plausible deniability of association with the group in the face of the direct consequences of the attack. As such, a smaller state may feel emboldened to try something in the cyber domain which it would otherwise not be able to accomplish via conventional military means – as a result, more powerful states can find themselves in a cyber struggle with a state they would likely disregard as a conventional military threat (Faesen et al, 2022). While the groups might be able to steal intellectual property or ransom data for financial gain, seeking state support for their activities can potentially allow them access to more sophisticated cyber tools (Merrigan, 2019). An example of this is the hacking group APT 17, which experts note conducts a range of economic, political, and military espionage activities for China (Merrigan, 2019).

V- ALLIED ADAPTION TO AN AGE OF CYBER CONFLICT

55. NATO's reckoning of the emergence of cyber attacks as a relevant topic for Allied security happened in several steps. From 2002 to 2016, NATO gradually built-up awareness for this challenge (Smeets, 2019). At the 2002 Prague Summit, Allies mentioned cyber attacks for the first time in their summit communiqué (Brent, 2019). Six years later, a first 'Policy on Cyber Defence' was adopted at the 2008 Bucharest Summit (Brent, 2019). Following the cyber attacks on Estonia in 2007, steps were thus taken at the summit to share best practices and support Allies in the case of emergencies relating to cyberspace. In 2012, Allies announced the operationalisation of its cyber rapid reaction teams, which Allies made available 24 hours a day to assist Allies with network security, capability development, as well as recovery in the event of a larger-scale cyber attack. The 2014 Wales Summit sparked the first debate around the role of cyber in relation to Article 5 of the North Atlantic Treaty and, as a result, whether to make it a core part of collective defence. Since then, NATO has acknowledged that a cyber attack could in fact lead to the invocation of Article 5.

56. Starting in 2016, NATO transitioned from a gradual reckoning of the cyber threat to a gradual operationalisation of cyber operations at NATO (Smeets, 2019). At the 2016 Warsaw Summit, Allies recognised cyberspace as a stand-alone domain of operations and issued a first Cyber Defence Pledge (Brent, 2019). The pledge recognised the need to "develop the fullest range of capabilities to defend [their] national infrastructures and networks" - particularly considering the Treaty's Article 3, relating to resilience (Smeets, 2019).

57. Two years later, at the 2018 Brussels Summit, NATO reaffirmed its commitment to the Pledge and announced the establishment of a Cyber Operations Centre (CyOC) (Smeets, 2019). The CyOC, located in Mons, Belgium, will be fully operational by 2023 (NATO, 2021). Its role is to provide a centralised space for situational awareness, coordination and planning of operations and mission (Brent, 2019). However, this does not mean NATO has changed its posture related to cyber - NATO personnel will not execute offensive cyber operations under the NATO flag (Lewis, 2019). Its approach to cyber remains purely defensive, with the sole caveat of allowing, if deemed necessary, the integration of "sovereign cyberspace effects from allies who are capable and willing to provide them" (Lewis, 2019). Several Allies have publicly stated they were prepared to do so, such as the United States, the United Kingdom, the Netherlands, Estonia, and Denmark (Lewis, 2019). This practice is in line with Allied contributions to NATO's activities in other domains - such as providing ships, tanks, or planes to the Alliance (Brent, 2019).

58. Following these developments, a NATO guide detailing tools to strengthen Allied ability to respond to cyber threats was published in February 2019 (NATO, 2022). The 2021 Brussels Summit saw the publication of a new 'Comprehensive Cyber Defence Policy', which "supports NATO's three core tasks of collective defence, crisis management and cooperative security, as well as its overall deterrence and defence posture" (NATO, 2022). The 2021 Summit also featured the increasing role of cyberspace for the Alliance prominently in its communiqué.

59. Several cyber-centric exercises allow NATO to deepen interoperability and test its concepts for cyberspace. *Cyber Coalition*, organised by Allied Command Transformation (ACT) is NATO's flagship cyber defence exercise, aiming to facilitate the combination of cyber effects provided by Allied nations (Brent, 2019). Other NATO exercises also include a distinct and growing cyber defence component, such as NATO HQ's *Crisis Management Exercise (CMX)* and *Trident Juncture* (Brent, 2019). The NATO-accredited Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, provides further ground for crucial education and training around cyberspace, notably through the organisation of the yearly *Locked Shields* and *Crossed Swords* exercises (Brent, 2019). To this end, Estonia also hosts a NATO Cyber Range (NATO, 2022).

60. NATO's Locked Shields 2022 ran from 19-22 April. The annual exercise took on increased significance this year, as Allies' cyber defences moved to high alert with Russia's invasion of Ukraine. As a pointed reminder of the exercise's significance Finland's government websites were attacked on 8 April in the heat of the country's political debate about joining NATO (Laikola, 2022). *Locked Shields* is the world's biggest and most complex real-time cyber defence exercise, the 2022 edition gathered more than 2,000 participants from over 33 nations (NATO, 2022(c)). This year's exercise placed teams in the role of a Cyber Rapid Reaction Team deployed to assist a fictional country with a large-scale cyber attack – from attribution to recovery. NATO Partner (currently in the process of acceding to the NATO Alliance) won the exercise, a joint Lithuanian-Polish team placed second, while Estonia came in third (NATO, 2022 (c)).

61. An array of other NATO policies, bodies, and agencies further support the Alliance's development and usage of cyber capabilities. The NATO Computer Incident Response Capability (NCIRC), affiliated with SHAPE in Mons, Belgium, acts as NATO's own emergency response team to mitigate direct threats to NATO information systems (NATO, 2022). Through the NATO Smart Defence Initiatives, Allies have established a Malware Information Sharing Platform (MISP) and a Smart Defence Multinational Cyber Defence Capability Development (MN CD2) (NATO, 2022). The NATO Communications and Information (NCI) Academy in Oeiras, Portugal, the NATO School in Oberammergau, Germany and on a more strategic level, the NATO Defense College in Rome foster technical and political understanding of cyber conflict issues for Allies and partners (NATO, 2022).

62. The cooperation with the European Union regarding cyberspace is also seen as a priority by the Alliance. NATO and the European Union are natural partners for cyber cooperation as they face common challenges but have different strengths to combat cyber challenges – together, they can amplify the effectiveness of their response. As a regulatory body, EU directed initiatives can align member states' priorities to advance the security of their national critical networks – some key developments in recent years do just that, for example: the Directive on Security of Network and Information Systems, which established the first set of EU-wide cybersecurity regulations; the Cyber Diplomacy Toolbox, seeking to offer member states a range of 'tools' to counter cyber threats; and, the EU Security Union Strategy and Screening of (Digital) investment; or, two key initiatives that resulted from the EU's Permanent Structured Cooperation (PESCO), the Cyber Threats and Incident Response Information Sharing Platform and the Cyber Rapid Response Teams (CRRTs); (Zandee, et. al., 2021; Bendiek, et. al., 2021).

63. In parallel, and following the 2016 Joint Declaration on NATO-EU Cooperation and a technical agreement between both parties, the breadth and depth of collaboration on "information exchange, training, research, and exercises" has deepened significantly. Cyber was listed as one of 74 areas of cooperation in the 2016 Joint Declaration, two years later, at the 2018 Brussels Summit, NATO Allies committed to raising the profile of cyber cooperation to make it a mutual policy priority. This has resulted in more joint exercising to build joint EU-NATO capacity to prevent cyber attacks against their member states, but also to be able to coordinate more effective reaction, recovery, and response when they do. As Deputy Assistant Secretary General for Emerging Security Challenges James Appathurai, noted at the June 2022 Microsoft European Cyber Agora, cooperation between NATO's and the EU's Cyber Incident Response Centers have been excellent for understanding the evolution and nature of cyber threats from which both organisations have benefitted significantly.

64. NATO also aims to foster partner cyber capabilities. Especially regarding Ukraine, NATO's support regarding cyber defence has been substantive – be it through the delivery of education and capacity building, the establishment of a NATO Trust Fund on Cyber Defence for Ukraine in 2014, the recent recommitment to increasing Ukraine's cyber defences amidst the ongoing war with Russia (NATO (b), 2022), or through Ukraine's recent accession to the CCDCOE (CCDCOE,

2022). In addition, NATO and the EU have established an informal, but very effective, platform to coordinate their cyber assistance to Ukraine. As the section above on the cyber elements of the Russia-Ukraine war makes clear, this has been critical to the defence of Ukraine, as defenders have thwarted attacks to allow for air defence systems to be maintained and basic services to continue at the time of the writing of this draft report.

VI- CYBER HIGH ON THE AGENDA OF THE MADRID SUMMIT

65. In the run-up to the June 2022 Summit of Heads of State and Government in Madrid, Spain, senior cyber coordinators from all NATO Allies met in Brussels on 18 May to review progress in collective efforts to bolster cyber defences, increase resilience, and deepen cooperation to share intelligence on evolving cyber threats, and coordinate response in the event of cyber attacks. This was the first such meeting and it helped shape Allies' cyber agenda for the summit. As a result, cyber-related issues were high on the summit agenda. The increased focus on cyber effects and network security is an implicit recognition of the interconnected nature of cyber and the significant potential for cyber effects to disrupt, deny, degrade, or destroy vital networks and systems upon which Allies' increasingly integrated defence and deterrence posture relies.

66. Allies set a new 'baseline' for their defence and deterrence posture in Madrid. To achieve this, Allies will build out a 'newly enhanced posture' in line with its already existing '360-degree approach, across the land, air, maritime, cyber, and space domains' (NATO, 2022(e)). NATO will build and support this higher baseline for defence and deterrence via the strengthening of Allies' approach to its three existing core tasks – deterrence and defence, crisis prevention and management, and cooperative security. The principal core task, Allies make clear in the Strategic Concept, is deterrence and defence. The other two tasks, in a way, fold on top of deterrence and defence, adding to its robustness and, woven throughout all three, Allies note in the Strategic Concept, is each Ally's individual and Allied collective commitment to improving their resilience.

67. Due to its inter-domain and tasking nature, it is no surprise that cyber defence capabilities and network resilience are considered vital to all three tasks as well as resilience initiatives. It is important to note, however, that cyber does feature as an important core element of the Alliance's broader deterrence and defence posture: "NATO's deterrence and defence posture is based upon an appropriate mix of nuclear, conventional and missile defence capabilities, complimented by space and cyber capabilities" (NATO, 2022(f)). Allies underscore the significant challenge they face in the cyber domain when they note in the description of the strategic environment they face today that "cyberspace is contested at all times" (NATO, 2022(f).

68. In line with cyber's crucial role in deterrence and defence, Allies pledge to 'expedite [their] digital transformation', requiring a focused adaptation of 'the NATO Command Structure for the information age and enhance our cyber defences, networks and infrastructure' (NATO, 2022(f)). New investments in innovative technologies will undergird the transition. More broadly, Allies understand the 'secure use and unfettered access to space and cyber are key to effective deterrence and defence' (NATO, 2022(f)). To guarantee this, Allies have decided, on a voluntary basis and using national assets, to build and exercise a virtual rapid response cyber capability to counter significant malicious cyber activities' (NATO, 2022(e)).

69. As Allies also make clear, cyber-related threats are a growing imperative with potentially far-reaching impact and response. They reaffirm in the Strategic Concept that: 'A single or cumulative set of malicious cyber activities…could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty' (NATO, 2022(f)). In response to the challenges of state conduct in cyberspace highlighted above, Allies also note in

the Strategic Concept that they 'recognise the applicability of international law and will promote responsible behaviour in cyberspace' (NATO, 2022(f)).

VII- CYBER ELEMENTS IN THE RUSSIA-UKRAINE WAR

70. The role of cyber, particularly the use of Russian cyber effects, during Russia's unprovoked invasion of Ukraine has been a keen focus of security analysts throughout the conflict. While some have been focusing on the 'cyber war that wasn't', others have noted the expected enabling role cyber operations have been playing in the broader military campaign, but some do fear Russia will deploy more destructive cyber operations as the conflict continues (Manjoo, 2022; Valeriano and Lonergan; 2022; Rid, 2022).

71. As noted above, while there certainly have not been, as some predicted, the spectacularly destructive surprises of a well-implemented cyber operation turning out the lights and causing communication systems chaos and more across Ukraine (Healey, 2022), Russian cyber operations have been a key element of the broader campaign. They were in fact part of the opening salvos of the conventional force invasion, on 23 and 24 February, as two malware 'wiper' attacks hit their targets, including a Ukrainian government network (Rid, 2022). It is hard to determine the tactical impact of the attacks, however, as the attacks were overshadowed by the growing destructiveness of Russia's conventional forces in Ukraine (Rid, 2022). In parallel to the ground invasion on 24 February, there was also a cyber attack on the ground infrastructure of the KA-SAT satellite, owned by the US company ViaSat, affecting 'high-value' communications of the Ukrainian military, police, and intelligence agencies (Burgess, 2022; Kavanagh, 2022). The impact of the satellite hack has also reverberated across Europe, from affecting wind turbine function in Germany to disrupting internet connectivity in France, Greece, Poland, Italy, and Hungary (Kavanagh, 2022).

72. Still, the reasons behind the relative dearth of larger-scale, destructive cyber attacks remain unclear. Some experts believe that once the conventional strikes began, the hard power destruction trumped the need for cyber operations that could turn out the lights in Ukraine (Halpern, 2022). One expert posits that, due to the secrecy surrounding the invasion, there was a lack of sufficient coordination between the Russian military and intelligence services and the related cyber and electronic warfare units (Moore, 2022). Other explanations note Russia's fear their attacks would impact their own forces' command and control abilities inside of Ukraine; or even that Russia lacked capabilities, or that those they did deploy failed to deliver (Kavanagh, 2022; Moore, 2022, Halpern, 2022). A common explanation, however, is the effectiveness of Ukrainian cyber defences played a major role in limiting the impact of Russian cyber operations in their broader military campaign.

73. Despite these successes, however, experts warn that the conflict is ongoing and cyber threats remain high and have the potential to have an impact on Allied interests and populations far more than they have already. As one expert notes, "As the pain of economic sanctions takes effect in Russia and tensions continue to rise dangerously, it is likely that we will see more activity targeting Ukraine, NATO, and EU countries" (Kavanagh, 2022). In addition, if Russia decides to increase cyber attacks on Ukraine as a means of further undermining Ukrainian morale as the conflict drags on, the nature of the networked world means that the chances for spill over also increase (Martin, 2022). Still, the nature of Russia's use of cyber effects in its campaign thus far relies on a strategy that, as a recent Microsoft analysis noted, "relies on in part on a cyber strategy that includes at least three distinct and sometimes coordinated efforts – destructive cyber attacks

within Ukraine, network penetration and espionage outside Ukraine, and cyber operations targeting people around the world" (Smith, 2022).

THE ESSENTIAL ROLE OF ALLIED AND PARTNER SUPPORT

74. Ukrainian cyber resilience in the face of Russia's cyber attacks is the result of key attention paid to the sector by the Ukrainian government after years of growing cyber bullying by Russia, as well as the critical external support from US Cyber Command, NATO Allies, the EU, as well as an array of private sector companies from across the US, Europe, and beyond (Valeriano and Lonergan, 2022; Halpern, 2022). This external assistance began in earnest after Russia's 2014 illegal annexation of Crimea and funnelling of financial and military support to the armed separatist formations it backs in eastern Ukraine. (NATO, 2022; Valeriano and Lonergan, 2022).

75. Since 2014, Ukraine has become the recipient of extensive partnership aid and cooperation with NATO Allies and their partners. NATO-Ukraine partnership has been perhaps the most extensive across all security sectors; the country's cyber capabilities and knowhow have been a key pillar of this cooperation. Several Trust Fund projects were launched in response to the 2014 Russia-Ukraine conflict; two focused on key areas essential to the development path toward strong cyber resilience and defences across all sectors of Ukraine, particularly within the armed forces – the C4 Trust Fund and the Cyber Defence Trust Fund. The C4 Fund worked along four key lines of effort to modernise C4 structures and capabilities to improve Ukraine's ability to defend itself and to increase interoperability with NATO Allies; they are regional airspace security, secure tactical communications, knowledge sharing, and situational awareness. The Cyber Defence Trust Fund focused on advanced technical abilities for cyber defence, including the establishment of an incident management centre and laboratories for monitoring cyber security incidents (NATO, 2022). The Cyber Trust Fund completed its tasks in 2017.

76. At the bilateral level, between 2014 and March 2022, the United States directed over USD 4 billion in State and Defense Department-funded security assistance to help reform and modernise Ukrainian defence institutions for both stronger stand-alone defence, but also to increase interoperability with US forces. The DOD-funded Ukraine Security Assistance Initiative allocated significant pre-war attention to building Ukrainian cyber defence and strategic communications to plug network vulnerabilities and counter Russian disinformation (Arabia, et, al., 2022).

77. When a large-scale cyber attack that struck Ukraine in June 2017 succeeded in shutting down government offices, banks, and even the postal service, Allies surged even more support to protect Ukraine's computer networks. Financial and technical support from the United States and NATO Allies sought to plug remaining vulnerabilities against determined and sophisticated Russian attacks (Halpern, 2022). In 2021, the United States military's Cyber Command deployed 'hunt forward' teams to Ukraine to identify threats to critical networks and assist their Ukrainian counterparts patch them (Volz, 2022). Assistance continued up to the invasion: as cyber attacks struck Ukrainian government websites in January in parallel to the troop build-up along Ukraine's borders, NATO Allies gave Ukraine access to the Alliance's malware information-sharing platform; in early February US Deputy National Security Adviser for Cyber and Emerging Technology, Anne Neuberger, travelled to Brussels and Warsaw to detail Russian cyber threats with officials from NATO, the EU, Poland and the Baltic countries; and, only days before Russia's invasion, the EU sent a Cyber Rapid Response Team to Ukraine (Halpern, 2022). As Viktor Zhora, deputy head of Ukraine's cyber-defence agency noted at a conference in late July, Allied cyber support in the lead-up to and just after the outbreak of the war "created a huge defensive force for Ukraine and…is one more reason we can continue to be resilient even during war" (Volz, 2022). Allied and partner efforts were also greatly assisted in their cyber intelligence by the additional efforts of private support to Ukraine.

78. As mentioned above, the public-private sector cooperation has proven essential to timely and vital cyber defence efforts in the Russia-Ukraine war. Just prior to the invasion on February 24, Microsoft's Threat Intelligence Center north of Seattle detected Russian-directed 'wiper' malware targeting Ukrainian ministries and financial institutions. The malware was quickly taken apart, named ('FoxBlade'), and the information on how to patch against passed on quickly to Ukraine's cyber defence authorities (Sanger, Barnes, Conger, 2022). After Microsoft executives communicated with the White House's deputy national security adviser for cyber and emerging technologies, the malware code's details were shared with Allies and partners across Europe to stymie the potential spread of the virus, which had the potential to have adverse impacts on Allied forces' capabilities or impair European banking systems (Sanger, Barnes, Conger, 2022).

79. Cyber experts believe Russia has already deployed the extent of its planned cyber weapons for its war efforts in Ukraine (Volz, 2022). Microsoft reporting on Russia's cyber operations suggest most Russia's cyber campaigns in the war thus far have focused on stealing information/battlespace espionage and the coordination of global influence campaigns to support their war efforts, rather than the incapacitation of networks (Smith, 2022). Early direct missile strikes on Ukraine's governmental data centre certainly had an impact, but this was minimised by Ukraine's pre-emption of this eventuality by disbursing and distributing the data across multiple networks both inside and outside the country with partner countries (Smith, 2022). This, coupled with sustained Allied and partner support, has allowed for the Ukrainian cyber forces to maintain their critical networks intact for effective continued operations. As such, some experts have concluded from the Russian experience in Ukraine that cyber attacks are unlikely to turn the tide of the war (Volz, 2022). Russia continues to not only probe for network vulnerabilities in Ukraine, but it has also increased its cyber espionage and attacks on Allied and partner nations assisting Ukraine (Smith, 2022).

80. Experts have noted the war's impact on Euro-Atlantic cyber cooperation, with some saying Allies and partners have entered a new era as a result (Volz, 2022). The war has pushed some Allies and partners to side line some existing technology policy disagreements in favour of breaking down the barriers to even closer cooperation – making the implementation of collective cyber security a policy imperative (Volz, 2022). NATO, the EU, and the UN are serving as key enabling platforms for this development. For example, the United States Cyber Command has noted it currently has 35 'hunt-forward' operations in 18 Allied countries – including Croatia, Estonia, Lithuania, Montenegro and the Republic of North Macedonia (Volz, 2022). These US deployed teams of cyber-defence personnel are often working in parallel on the ground with their EU and NATO cyber rapid reaction teams. In addition to this, Allies and partners have been instrumental to recent progress in a United Nations working group focusing on developing international cyber security standards.

VIII- CONCLUSIONS FOR NATO PARLIAMENTARIANS

81. Understanding the impact of the rapid evolution of the cyber domain is essential for NATO Parliamentarians. Increased digital dependence across almost every sector of modern life is, in parallel, also increasing the cyber threat surface and, therefore, potential reach and impact of cyber attacks. As Allies noted in their 2021 Summit Declaration, "Cyber threats to the security of the Alliance are complex, destructive, coercive, and becoming ever more frequent" (NATO, 2021).

82. Modern militaries are particularly wired; their forces' platforms running on ever more sophisticated software and interdependent for battlefield manoeuvre, understanding, and mission execution. Efforts to exploit the potential weaknesses in these modern systems have given rise to

sophisticated cyber warfare effects across most modern nations, as well as the electronic warfare means to try and thwart them.

83. As the Alliance faces an era of increased competition with assertive and authoritarian powers, particularly Russia and China, it is clear the cyber domain will be an increasingly contested domain. While Russia and China seek the ways and means to achieve 'cyber sovereignty', they engage in near constant efforts to compromise Allies' systems to pilfer intellectual property and steal state secrets, put critical infrastructure at risk, and subvert and undermine democratic institutions. They are also building out the cyber effects to ensure they have the capability to deploy cyber operations in support of a potential broader military struggle in the future. As such, the risks of weak cyber defences and deficient cyber effects pose potentially sweeping damages to Allies' core interests.

84. NATO Allies have recognised this risk and adopted the Cyber Defence Pledge in 2016 to maintain strong national cyber defence policies a priority for all Allies. The 2021 Comprehensive Cyber Defence Policy in support of NATO's three core tasks of collective defence, crisis management, and cooperative security further reinforced this Alliance-wide commitment to remain focused on maintaining the most advanced cyber defence capabilities. The impact of NATO's cooperative cyber security outreach has been on display in the current Russia-Ukraine war, as Ukraine's cyber defences – rebuilt and supported with Allied assistance – have significantly mitigated the impact of cyber attacks over the course of the war.

85. Still, more can and should be done. This report advocates the following key measures:

- **Continued and increased investment in the interoperability of Allied cyber forces.** Allies have to expect that cyber conflict – both in warfare and measures short of warfare – will expand both in volume and intensity in the coming decades. To that end, the creation of the NATO CyOC in 2018 is a crucial step that was already taken. Yet, such a unit can only function at maximum efficiency if Allies deepen the pooling of intelligence and establishing of common practices and methods for the interoperability of cyber effects. To enhance NATO's deterrence in cyberspace, more Allies could publicly state they are ready to delegate their sovereign cyber effects to NATO operations should such a need arise.
- **Extended dialogue with key actors of the private sector.** Many crucial nodal points for data and information flows in cyberspace are under the responsibility of private actors in the information and communication technologies field. Social network and other software companies thus often have access to real-time information on cyber conflict public actors might not have. While staying mindful of existing privacy and surveillance laws, deepening collaboration with these actors will thus become a key enabler to a more resilient cyber defence.
- **Create the domestic legal frameworks allowing for fast and effective response to cyber incidents as an Alliance.** Cyber incidents bear an increased risk of spreading beyond borders indiscriminately. NATO and Allied communication could also be targeted as a whole. It is thus a necessity to bolster the common response of Allies for cyber incidents – both in the speed and coordination of incident response, as well as in the subsequent attribution of cyber incidents. Since attribution of cyber attacks is a political act, strengthening NATO's role as a platform to do this would enhance the credibility of the findings.
- **Foster more coherent and resilient legal systems regarding cyberspace across the Alliance.** NATO Parliamentarians have a special duty to ensure that their domestic legal frameworks are well adapted to the new challenges posed by cyber conflict. The NATO CCDCOE's Tallinn manual 2.0 on the international law applicable to cyber operations offers avenues to think about the current international dimensions of cyber

conflict. Yet, many of these elements should also flow back into the domestic legislative system – or spark a common debate among Allies – to establish a more coherent line. Allied Parliamentarians should thus think about how they can foster a better common understanding of practices such as the buying and exploiting of zero-days for national security purposes; the legal frameworks around private actors carrying out cyber effects or the prosecution of cyber criminals abroad that may or may not be tied to adversary cyber operations.

- **Continue to engage in extensive cyber cooperation with partners.** As this report highlights, the targeted outreach programmes with Ukraine from 2014 to the present day proved effective at thwarting significant Russian cyber operations and mitigating the impact of those that made it through. Working in tandem with international partners, such as the EU, NATO can multiply the impact of its partnership outreach. Increased attention to programmes with potentially vulnerable partners such as Georgia and Moldova, for instance, can help forestall the potential consequences of increased cyber operations in these nations.
- **Redouble efforts to sustain Ukraine's cyber defences.** In line with the last recommendation, Allies must also commit to even more support for Ukraine's cyber defence effects as they face a constant barrage of cyber assaults from Russia. Together with continued financial, diplomatic, humanitarian, and military support, increased flow of cyber support to Ukraine will go a long way to helping the Ukrainian people overcome Russia's savage and unprovoked attack on their sovereignty.
- **Support the cyber initiatives of the Madrid Summit and Strategic Concept**. As the report makes clear, Allies made bold and important pledges vis-à-vis reaching a new deterrence and defence baseline at the Madrid Summit. There is no doubt such an ambition will include significant new funding to continue to adapt NATO Command and Control structure to cutting edge information age requirements. This means not only new critical cyber networks and systems, but also the means to defend them. It also means, however, that all Allies must look more closely at the ways and means to continue to upgrade and adapt their own national networks and capabilities, as this will be a key element of the much-needed focus on whole-of-Alliance resilience necessary to underpin and safeguard the Alliance's new deterrence and defence posture. NATO parliamentarians must advocate for these required new investments with their national governments. They must also remember that higher Alliance and national deterrence and defence ambitions require enduring political will to sustain them.

Draft

BIBLIOGRAPHY

Acton, James M. 'Cyber Weapons and Precision-Guided Munitions – Understanding Cyber Conflict: 14 Analogies.' Carnegie Endowment for International Peace. 16 October 2017. https://carnegieendowment.org/2017/10/16/cyber-weapons-and-precision-guided-munitions-pub-73397.

Aday S., Andžāns M., Bērziņa-Čerenkova U., Granelli F., Gravelines J., Hills M., Holmstrom M., Klus A., Martinez-Sanchez I., Mattiisen M., Molder H., Morakabati Y., Pamment J., Sari A., Sazonov V., Simons G., Terra J. 'Hybrid Threats: 2007 cyber attacks on Estonia' in *Hybrid Threats. A Strategic Communications Perspective*. Riga: NATO Strategic Communications Centre of Excellence. 2019. https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

Agbebi, Motolani. 'China's Digital Silk Road and Africa's Technological Future.' Council on Foreign Relations, 1 February 2022. https://www.cfr.org/blog/chinas-digital-silk-road-and-africas-technological-future.

Alami, Mona. 'Russia's Disinformation Campaign Has Changed How We See Syria.' Atlantic Council, 4 September 2018. https://www.atlanticcouncil.org/blogs/syriasource/russia-s-disinformation-campaign-has-changed-how-we-see-syria.

Arabia, Christina, Andrew Bowen, and Cory Welt, "U.S. Security Assistance to Ukraine," Congressional. Research Service, Updated 29 April 2022. https://crsreports.congress.gov/product/pdf/IF/IF12040

Arquilla, John, 'Bitskrieg: The New Challenge of Cyberwarfare'. Polity Press. 2021.

Austin, Greg. 'How Good are China's Cyber Defenses?' The Diplomat, 11 July 2018. https://thediplomat.com/2018/07/how-good-are-chinas-cyber-defenses.

BBC. 'Putin: Patriotic Russians May Be Involved in Hacking. BBC News, 1 June 2017. https://www.bbc.com/news/technology-40122943

Bendiek, Annegret and Matthias Schulze. 'Attribution: A Major Challenge for EU Cyber Sanctions.' German Institute for International and Security Affairs, December 2021. https://www.swp-berlin.org/en/publication/attribution-a-major-challenge-for-eu-cyber-sanctions.

Bendiek, Annegret and Matthias C. Kettemann, "Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy," Stiftung Wissenschaft und Politik (SWP) German Institute for International and Security Affairs, February 2021. https://www.swp-berlin.org/publications/products/comments/2021C16_EUCyberDiplomacy.pdf

Bigelow, Brad. 'What are Military Cyberspace Operations Other Than War?'11th International Conference on Cyber Conflict (CyCon), 1–17. 2019. https://doi.org/10.23919/CYCON.2019.8756835.

Boeke, Sergei, & Broeders, Dennis. 'The Demilitarisation of Cyber Conflict'. Survival, 60(6), 73–90. 2018. https://doi.org/10.1080/00396338.2018.1542804.

Bowen, Andrew S. 'Russian Cyber Units'. *Congressional Research Service*, 4 January 2021, 3.

Brent, Laura. 'NATO's role in cyberspace'. NATO Review. 12 February 2019. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

Brumfield, Cynthia. 'Common Pitfalls in Attributing Cyberattacks.' CSO, 16 October, 2020. https://www.csoonline.com/article/3584870/common-pitfalls-in-attributing-cyberattacks.html.

Buchanan, Ben., Schmidle Jr, Robert E., & Sulmeyer, Michael. 'Nonlethal Weapons and Cyber Capabilities – Understanding Cyber Conflict: 14 Analogies.' Carnegie Endowment for International Peace. 16 October 2017. https://carnegieendowment.org/2017/10/16/nonlethal-weapons-and-cyber-capabilities-pub-73396.

Burgess, Matt, "A Mysterious Satellite Attack Has Victims Far Beyond Ukraine," *Wired*, 23 March 2022. https://www.wired.com/story/viasat-internet-hack-ukraine-russia/

Canadian Centre for Cyber Security. 'An Introduction to the Cyber Threat Environment'. Canadian Centre for Cyber Security, 2020. https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment.

CCDCOE. 'Ukraine to be accepted as a Contributing Participant to NATO CCDCOE'. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). 4 March 2022. https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/.

Chang, Amy. 'Warring State: China's Cybersecurity Strategy.' Center for a New American Security, December 2014. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS_WarringState_Chang_report_010615.pdf?mtime=20160906082142&focal=none.

Cheng, Dean. 'Winning Without Fighting: The Chinese Psychological Warfare Challenge.' Heritage Foundation, 12 July 2013. https://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge.

China Aerospace Studies Institute. 'In Their Own Words: Foreign Military Thought.' China Aerospace Studies Institute, 8 February 2021. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf.

China Internet Network Information Center. 'Statistical Report on Internet Development in China. September 2020. http://www.cnnic.com.cn/IDR/ReportDownloads/202012/P020201201530023411644.pdf.

CISA. 'Security Tip (ST04-001). What is Cybersecurity?', 14 November 2019. https://www.cisa.gov/uscert/ncas/tips/ST04-001.

Connell, Michael, & Vogler, Sarah. 'Russia's Approach to Cyber Warfare' ©, 29. 2017. https://www.cna.o©can_files/pdf/DOP-2016-U-014231-1Rev.pdf

CSIS. 'Survey of Chinese Espionage in the United States Since 2000.' Center for Strategic and International Studies. https://www.csis.org/programs/technology-policy-program/survey-chinese-linked-espionage-united-states-2000.

Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata. 'Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War.' Security Dialogue, Vol. 42, no. 1, February 2012. https://www.jstor.org/stable/26301960.

Denning, Dorothy and Bradley Strawser. 'Active Cyber Defense: Applying Air Defense to the Cyber Domain', in 'Understanding Cyber Conflicts: 14 Analogies'. Georgetown University Press. 2017. https://carnegieendowment.org/2017/10/16/understanding-cyber-conflict-14-analogies-pub-72689

DeSombre, Winnona, Shires, James, Work, JD, Herr, Trey, & Morgus, Robert. 'A primer on the proliferation of offensive cyber capabilities'. Atlantic Council. 1 March 2021. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/.

Ding, Jeffrey. 'Technology, Trade, and Military – Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy.' US-China Economic and Security Review Commission, 7 June 2019. https://www.uscc.gov/hearings/technology-trade-and-military-civil-fusion-chinas-pursuit-artificial-intelligence-new.

Eaglen, Mackenzie. 'The Forge Software Factory is in Need of Stable Resourcing'. Defense News. 24 January 20212.

Egloff, Florian J. 'Semi-State Actors in Cybersecurity'. *Oxford University Press*. 2022.

Egloff, Florian J. 'Why Do States Publicly Attribute Cyber Intrusions?' Council on Foreign Relations, 14 October 2020. https://www.cfr.org/blog/why-do-states-publicly-attribute-cyber-intrusions.

Egloff, Florian J. and Andreas Wenger. 'Public Attribution of Cyber Incidents.' Center for Security Studies ETH Zurich, May 2019. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse244-EN.pdf.

Economy, Elizabeth C. 'The Great Firewall of China: Xi Jinping's Internet Shutdown.' The Guardian, 29 June 2018. https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.
Eichensehr, Kristen. 'Cyberattack Attribution and International Law.' Just Security, 24 July 2020. https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law.
Faesen, Louk, Tim Sweijs, Alexander Klimburg, and Giulia Tesauro . "The PrPromises and Perils of a Minimum Cyber Deterrence Posture: Considerations for Small and Middle Powers ." Hague Center for Strategy Studies, April 6, 2022. https://hcss.nl/report/promises-and-perils-of-minimum-cyber-deterrence-posture/.
Florant, Jean-Baptiste. 'Cybe rar mes: La lutte informatique offensive dans la manœuvre future.' IFRI. January 2021. https://www.ifri.org/fr/publications/etudes-de-lifri/focus-strategique/cyberarmes-lutte-informatique-offensive-manoeuvre.
Friedman, Allan and P.W. Singer, Cybersecurity and Cyberwar: What Everyone Needs to Know'. Oxford University Press. 2014.
Greenberg, Andy. 'Hackers Tied to Russia's GRU Targeted the US Grid for Years.' Wired. 24 February 2021. https://www.wired.com/story/russia-gru-hackers-us-grid/.
Guerrero-Saade, Juan Andres, Raiu, Costin, Moore, Daniel, & Rid, Thomas. 'Penquin's Moonlit Maze. The Dawn of Nation-State Digital Espionage'. Kaspersky. 2017. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf.
Hakala, Janne and Jazlyn Melnychuk. 'Russia's Strategy in Cyberspace'. NATO Strategic Communications Centre of Excellence, June 2021. https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210.
Halpern, Sue. "The Threat of Russian Cyber Attacks Looms Large," *The New Yorker*, 22 March 2022.
Healey, Jason, "Preparing for Inevitable Cyber Surprise," *War on the Rocks*, 12 January 2022. https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/
Ho, Matt. 'China's Hi-Tech Direction for the Next Five Years.' South China Morning Post, 11 November 2020. https://www.scmp.com/news/china/politics/article/3109316/chinas-hi-tech-direction-next-five-years.
Howell O'Neill, Patrick. 'A patient has died after ransomware hackers hit a German hospital.' MIT Technology Review. September 18 2020. https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital/.
ICC. 'ICC Policy Primer on Cybersecurity'– *I–C - International Chamber of Commerce* (blog), June 2021. https://iccwbo.org/publication/icc-policy-primer-on-cybersecurity/.
IISS. 'Cyber Capabilities and National Power: A Net Assessment'. IISS, 28 June 2021. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.
Jacobsen, Jeppe T. 'Cyber offense in NATO: Challenges and opportunities'. International Affairs, 97(3), 703–720. 2021. https://doi.org/10.1093/ia/iiab010.
Jibilian, Isabella and Katie Canales. 'The US is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of how the Massive Hack Happened and Why it's Such a Big Deal.' Business Insider, 15 April 2021. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T.
Jing de Jong-Chen. 'China's Evolving Cybersecurity and Cyber Development Strategy.' National Bureau of Asian Research, 29 March 2017. https://www.nbr.org/publication/chinas-evolving-cybersecurity-and-cyber-development-strategy.
Kaspersky. 'Cyber Attribution.' Kaspersky IT Encyclopedia. https://encyclopedia.kaspersky.com/glossary/cyber-attribution.
Kastelic, Andraz. 'Non-Escalatory Attribution of International Cyber Incidents.' United Nations Institute for Disarmament Research, 6 January 2022. https://www.unidir.org/publication/non-escalatory-attribution-international-cyber-incidents.

Kavanagh, Camino. 'Ukraine: Cyber Operations and Digital Technologies'. Directions Blog. 22 March 2022. https://directionsblog.eu/ukraine-cyber-operations-and-digital-technologies/.
Kennedy, Scott. 'Made in China 2015.' Center for Strategic and International Studies, 1 June 2015. https://www.csis.org/analysis/made-china-2025.
Klein, Roland. "Trimming P'ga'us' Wings." Völkerrechtsblog, October 27, 2021. https://voelkerrechtsblog.org/de/trimming-pegasus-wings/.
Kolton, Michael. 'Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence.' The Cyber Defense Review, Vol. 2, No. 1, 2017. https://www.jstor.org/stable/pdf/26267405.pdf.
Kuerbis, Brenden et al. 'Understanding Transnational Cyber Attribution: Moving From "Whodunit" to Who Did It.' Routledge (London), 16 February 2022. https://www.taylorfrancis.com/books/oa-edit/10.4324/9781003110224/cyber-security-politics-myriam-dunn-cavelty-andreas-wenger.
Kurlantzick, Joshua. 'As China Extends Its Reach Abroad, When Does Influence Become Interference.' World Politics Review, 8 January 2018. https://www.worldpoliticsreview.com/articles/23935/as-china-extends-its-reach-abroad-when-does-influence-become-interference.
Kushner, David. 'The real sto24tuxnettuxnet.' IEEE Spectrum, 50(3), 48–53. 2013. https://doi.org/10.1109/MSPEC.2013.6471059.
Laikola, Leo, "Finland Hit by Cyber Attack, Airspace Breech as NATO Bid Weighed," Bloomberg, 8 April 2022. https://www.bloomberg.com/news/articles/2022-04-08/finland-hit-by-cyber-attack-airspace-breach-as-nato-bid-weighed
Lewis, Don. 'What is Nato Really Doing in Cyberspace?'. War On The Rocks. 4 February 2019. https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/.
Lu, Christina. 'China's Social Media Explosion.' Foreign Policy, 11 November 2021. https://foreignpolicy.com/2021/11/11/china-social-media-tech-linkedin-wechat-censorship-privacy-regulation.
MacAskill, Ewen. 'Cyber-attack risk on nuclear weapons systems 'relatively high' – thinktank'. The Guardian. 11 January 2018. https://www.theguardian.com/technology/2018/jan/11/cyber-attack-risk-on-nuclear-weapons-systems-relatively-high-thinktank.
Machi, Vivienne. 'NATO looking at holistic path to boost cyber defense arsenal'. Defense News, 14 December 2021. https://www.defensenews.com/global/europe/2021/12/14/nato-looking-at-holistic-path-to-boost-cyber-defense-arsenal/.
Manjoo, Farhad. 'The Ukranian Cyberway that Wasn't'. The New York Times, 11 March 2022. https://www.nytimes.com/2022/03/11/opinion/russia-ukraine-cyberattacks.html
Markoff, John. 'Before the Gunfire, Cyberattacks.' New York Times, 12 August 2008. https://www.nytimes.com/2008/08/13/technology/13cyber.html.
Martin, Ciaran. 'Cyber Realism in a Time of War'. Lawfare Blog. 2 March 2022. https://www.lawfareblog.com/cyber-realism-time-war.
McBride, James and Andrew Chatzky. 'Is "Made in China 2025" a Threat to Global Trade?' Council on Foreign Relations, 13 May 2019. https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.
McReynolds, Joe. 'China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy.' China Brief, vol. 15, no. 8, April 2015. https://jamestown.org/program/chinas-evolving-perspectives-on-network-warfare-lessons-from-the-science-of-military-strategy.
McDermott, Roger. 'Russia's Electronic Warfare Capabilities as a Threat to GPS.' The Jamestown Foundation, 10 March 2021. https://jamestown.org/program/russias-electronic-warfare-capabilities-as-a-threat-to-gps.
Merrigan, Elizabeth. "Blurred Lines between State and Non-State Actors." Council on Foreign Relations. Council on Foreign Relations, December 5, 2019. https://www.cfr.org/blog/blurred-lines-between-state-and-non-state-actors.

Moore, Daniel. 'Some thoughts on offensive cyber ops (OCOs) & influence campaigns in the context of Ukraine. Both potential and reality'. Twitter. 28 February 2022. https://threadreaderapp.com/thread/1498421362863624194.html.
Nakashima, Ellen. 'Russian Military was Behind "NotPetya" Cyberattack in Ukraine, CIA Concludes.' Washington Post, 12 January 2018. 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.
NATO. 'Cyber defence'. NATO. 23 March 2022. https://www.nato.int/cps/en/natohq/topics_78170.htm.
NATO(b), "Deputy Secretary General stresses NATO will continue to increase Ukraine's cyber defences," 25 January 2022. https://www.nato.int/cps/en/natohq/news_191143.htm.
NATO (c), "NATO Allies and Partners Participate in Large-Scale Cyber Defence Exercise," 29 April 2022. https://www.nato.int/cps/en/natohq/news_194902.htm?selectedLocale=en
NATO(d), "Statement by the North Atlantic Council Concerning the Malicious Cyber Activities Against Albania," Pres Release, 8 September 2022. https://www.nato.int/cps/en/natohq/official_texts_207156.htm
NATO(e), Madrid Summit Declaration, issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022.
NATO (f) NATO 2022 Strategic Concept.
NATO, 'Factsheet: NATO Cyber Defence' NATO April 2021 https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf.
NATO, 'Brussels Summit Communiqué', 14 June 2021. https://www.nato.int/cps/en/natohq/news_185000.htm
NTI. 'Addressing Cyber-Nuclear Security Threats'. Nuclear Threat Initiative. 2019. https://www.nti.org/about/programs-projects/project/addressing-cyber-nuclear-security-threats/.
Nye, Joseph, 'Cyber Power'. The Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010.
Osborn, Kris, 'Navy Tests Stealth Zumwalt Destroyer Computers'. Defense Systems. 9 April 2017. https://defensesystems.com/cyber/2017/04/navy-tests-stealth-zumwalt-destroyer-computers/189051/
Perlroth, Nicole, and Sanger, David. "Hacks Raise Fear over '.S.A.'s Hold on Cyberweapons." The New York Times. The New York Times, June 29, 2017. https://www.nytimes.com/2017/06/28/technology/ransomware-nsa-hacking-tools.html.
Perlroth, Nicole. "How the United States Lost to Hackers." The New York Times. The New York Times, February 6, 2021. https://www.nytimes.com/2021/02/06/technology/cyber-hackers-usa.html.
Pinchuk, Denis. 'Patriotic Russians May Have Staged Cyber Attacks on Own Initiative: Putin.' Reuters, 1 June 2017. https://www.reuters.com/article/us-russia-economic-forum-putin-cyber-idUSKBN18S56Y.
Reuters, "Albania Cuts Iran Ties Over Cyberattack, U.S. Vows Further Action," 7 September 2022. https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/
Rid, Thomas, & McBurney, Peter. 'Cyber-Weapons'. The RUSI Journal, 157(1), 6–13. 2012. https://doi.org/10.1080/03071847.2012.664354.
Rid, Thomas. 'Why You Haven't Heard About the Secret Cyberwar in Ukraine'. New York Times. 18 March 2022. https://www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html.
Sanger, David. 'Confront and Conceal:'Obama's Secret Wars and Surprising Use of American Power' Crown Publishing. 2012.

Sanger, David, Julian Barnes and Kate Conger. 'As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War.' New York Times. 28 February, 2022. https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html.
Sanger, David, & Perlroth, Nicole. 'U.S. Escalates Online Attacks on Russia's Power Grid.' The New York Times. 15 June 2019. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.
Sacks, Samm and Robert O'Brien. 'What to Make of the Newly Established Cybersecurity Association of China.' Center for Strategic and International Studies, 25 May 2016. https://www.csis.org/analysis/what-make-newly-established-cybersecurity-association-china.
Savic, Misha, "Ransomware Attack Sends Montenegro Reaching Out to NATO Partners," Bloomberg, 1 September 2022. https://www.bloomberg.com/news/articles/2022-09-01/ransomware-attack-sends-montenegro-reaching-out-to-nato-partners?leadSource=uverify%20wall
Security Council of the Russian Federation, "Doctrine of Information Security of the Russian Federation," 2016. http://www.scrf.gov.ru/security/information/DIB_engl/
Segal, Adam. 'China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace.' The National Bureau of Asian Research, Special Report no. 87. https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace.
Segal, Adam and Lorand Laskai. 'A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage.' Council on Foreign Relations, 6 December 2018. https://www.cfr.org/report/threat-chinese-espionage.
Slayton, Rebecca. 'Why Cyber Operations Do Not Always Favor the Offense. Belfer Center for Science and International Affairs.' February 2017. https://www.belfercenter.org/publication/why-cyber-operations-do-not-always-favor-offense.
Smeets, Max. 'NATO's Cyber Policy 2002-2019: A very, very brief overview'. Max Smeets. 2 December 2019. http://maxsmeets.com/2019/12/natos-cyber-policy-between-2002-2019-a-very-very-brief-overview/.
Snegovaya, Maria. 'Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare.' Institute for the Study of War, September 2015. https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.
Solomon, Howard. 'Experts Say Worldwide Cost of Investigating SolarWinds Orion Hack Could Be in the Billions.' IT World Canada, 11 January, 2021. https://www.itworldcanada.com/article/world-wide-cost-of-investigating-solarwinds-orion-hack-could-be-100-billion-says-one-estimate/440507.
Smith, Brad, "Defending Ukraine: Early Lessons from the. Cyber War," Microsoft, 22 June 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK
Spindel, Jennifer. "Artificial Intelligence and Nuclear Weapons: Bringer of Hope or Harbinger of Doom?" European Leadership Network, August 17, 2020. https://www.europeanleadershipnetwork.org/commentary/bringer-of-hope-or-harbinger-of-doom-artificial-intelligence-and-nuclear-weapons/.
Stacey, Ed. 'Future Warfighting in the 2030s: An Interview with Franz-Stefan Gady.' Strife. 9 September 2020. https://www.strifeblog.org/2020/09/09/future-warfighting-in-the-2030s-an-interview-with-franz-stefan-gady/.
State Council of the People's Republic of China. 'Notice of the State Council Issuing the New Generation of Artificial Intelligence Development Plan.' State Council Document no. 35, 8 July 2017. https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf.
Stevens, Tim. 'Cyberweapons: An emerging global governance architecture.' Palgrave Communications, 3(1), 16102. 2017. https://doi.org/10.1057/palcomms.2016.102.

Stiennon, Richard, "A Short History of Cyber Warfare," in James A. Green, Cyber Warfare: A Multidisciplinary Analysis, Routledge, 2015. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315761565-2/short-history-cyber-warfare-richard-stiennon

Sway. 'Are we ready for Putin's Cyber War? I asked One of Biden's Top Cybersecurity Officials'. New York Times. 10 March 2022. https://www.nytimes.com/2022/03/10/opinion/sway-kara-swisher-anne-neuberger.html.

Swinhoe, Dan. 'How much does it cost to launch a cyberattack?' CSO Online. 1 May 2020. https://www.csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html.

Tashev, Blagovest, Michael Purcell, and Brian McLaughlin. 'Russia's Information Warfare: Exploring the Cognitive Dimension.' MCU Journal, Vol. 10, no. 2. Fall 2019. https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/MCU-Journal-Fall-2019/#:~:text=Russia's%20Information%20Warfare%3A,Exploring%20the%20Cognitive%20Dimension&text=Abstract%3A%20The%20U.S.%20military%20increasingly,disrupting%20adversaries%20and%20other%20groups.

UK National Cyber Security Centre. 'Advisory: Turla group exploits Iranian APT to expand coverage of victims'. NCSC, 21 October 2019. https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims.

US DOD. 'Joint Publication 3-12. Cyberspace Operations', 8 June 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

Valeriano, Brandon and Erica D. Lonergan. 'What Ukraine Shows about Cyber Defense and Partnerships'. Cato Institute. 17 March 2022. https://www.cato.org/commentary/what-ukraine-shows-about-cyber-defense-partnerships.

van der Waag-Cowling, Noëlle. 'Stepping into the breach: Military responses to global cyber insecurity.' Humanitarian Law & Policy Blog. 17 June 2021. https://blogs.icrc.org/law-and-policy/2021/06/17/military-cyber-insecurity/.

Veale, Michael, and Ian Brown. 'Cybersecurity'. *Internet Policy Review* 9, no. 4 (17 December 2020). https://doi.org/10.14763/2020.4.1533.

Vermes, Jason. 'There's Another Conflict Happening Between Russia & Ukraine — an Information War That's Been Waging for Years.' CBC, 13 December 2021. https://www.cbc.ca/radio/day6/russian-propaganda-best-bad-xmas-movies-west-side-story-s-lgbtq-roots-emmett-till-s-cousin-and-more-1.6280485/there-s-another-conflict-happening-between-russia-ukraine-an-information-war-that-s-been-waging-for-years-1.6280496.

Volz, Dustin, "Russia's War on Ukraine Deepens International Cyber-Defense Cooperation," *The Wall Street Journal*, 6 September 2022.

White House, "Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania," Briefing Room, Statements and Releases, 7 September 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/

White, Sarah P. 'Understanding Cyberwarfare: Lessons from the Russia-Georgia War.' Modern War Institute, 30 March 2018. https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/.

Wolff, Josephine. 'Understanding Russia's Cyber Strategy'. FPRI, 6 July 2021. https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/.

Woolley, Pamela L. 'Defining Cyberspace as a United States Air Force Mission.' Air Force Institute of Technology, June 2006. https://apps.dtic.mil/sti/citations/ADA453972.

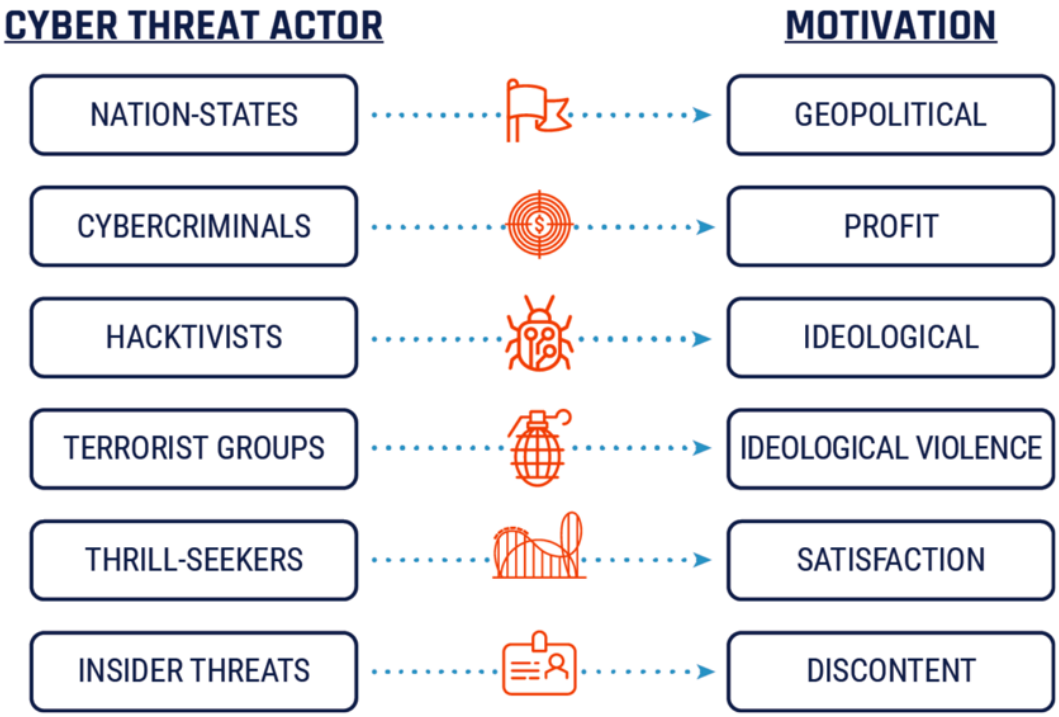
Ying, Jiang. 'Chinese Anger with Western Media's Assumptions of Political Change.' University of Adelaide Press, 2012. https://www.jstor.org/stable/10.20851/j.ctt1sq5x62.10?seq=1#metadata_info_tab_contents.

Yuan, Li. 'A Generation Grows Up in China Without Google, Facebook or Twitter.' New York Times, 6 August 2018. https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-internet.html.
Zhang, Longmei and Sally Chen. 'China's Digital Economy: Opportunities and Risks.' IMF, January 2019. https://www.imf.org/en/Publications/WP/Issues/2019/01/17/Chinas-Digital-Economy-Opportunities-and-Risks-46459.
Zandee, Dick, Sico Van Der Meer, and Adaja Stoetman, "Countering Hybrid Threats: Steps for Improving NATO-EU Cooperation," Clingendael – Netherlands Institute of International Relations, October 2021.

ANNEXES

ANNEX 1: CYBER THREAT ACTORS AND MOTIVATIONS

Figure 1: Cyber threat actors



(Source: CCCS, 2020)

ANNEX 2: THE FIVE PILLARS OF OFFENSIVE CYBER CAPABILITY PROLIFERATION

TABLE 1. THE FIVE PILLARS OF OFFENSIVE CYBER CAPABILITY PROLIFERATION

	Definition	Government examples	Criminal examples	industry examples	AaaS examples
VULNERABILITY RESEARCH AND EXPLOIT DEVELOPMENT	Discovered vulnerabilities, or disclosure programs that facilitate the proliferation of discovered vulnerabilities and written exploits	Chinese intelligence community vulnerability research and exploitation, specifically within the MSS and its associated CNNVD	Exploit kits sold on underground forums	Bug bounty programs, vulnerability disclosures, Zerodium	NSO Group's use of a WhatsApp 0day
MALWARE PAYLOAD DEVELOPMENT	Any malware or tool written or used by attackers to conduct offensive cyber operations, or any forum that encourages or conducts exchange of malware	Custom malware developed by state teams that is reverse engineered and published by malware analysts	Commercial malware market	Red-team tools developed and sold through commercial offerings and companies; posting malware for research on GitHub	NSO Group's Pegasus spyware
TECHNICAL COMMAND AND CONTROL	Technologies aimed at supporting offensive cyber operations, e.g., bulletproof hosting, domain name registration, server side command-and-control software, VPN services, or delivery accounts involved with the initial creation of an offensive cyber operation	IPs and domains attributed to state operations by threat intelligence reports	Bulletproof hosting and other pre-bullet command-and-control infrastructure	Test servers built to send phishing tests against one's own companies, infrastructure used for penetration testing services	Infrastructure used by Appin Security for Operation Hangover
OPERATIONAL MANAGEMENT	Operations management, strategic organization of resources and teams, initial targeting decisions, and other functions that are required to effectively manage an organization that conducts cyber operations	Chain of command within and organization of government intelligence agencies	Criminal outsourcing, ransomware affiliate programs	Delegation of duties within a red-team exercise; escalation policies during an incident	Good Harbor Consulting's organizational management of UAE DREAD cyber capabilities
TRAINING AND SUPPORT	Training or education provided on the offensive cyber operation process, expanding the number of trained professionals and creating connections between them that facilitate the growth of OCC	NSA's National Cryptologic School or other government-sponsored cyber training program	Fraud tutorials, phishing kits, customer support provided within forums	Kali Linux tutorials on YouTube, cyber security certifications, conference trainings and talks	DarkMatter training provided to UAE cyber operators

Note: Abbreviations: MSS: China's Ministry of State Security; CNNVD: China's National Vulnerability Database; AaaS: Access-as-a-Service; VPN: virtual private network; IP: Internet Protocol; OCC: offensive cyber capabilities; UAE: United Arab Emirates; DREAD: the UAE's Development Research Exploitation and Analysis Department; NSA: US National Security Agency.

(*Source*: DeSombre et al., 2021)