NATO PARLIAMENTARY ASSEMBLY
ASSEMBLEE PARLEMENTAIRE DE L'OTAN

COMMITTEE ON DEMOCRACY AND SECURITY (CDS)

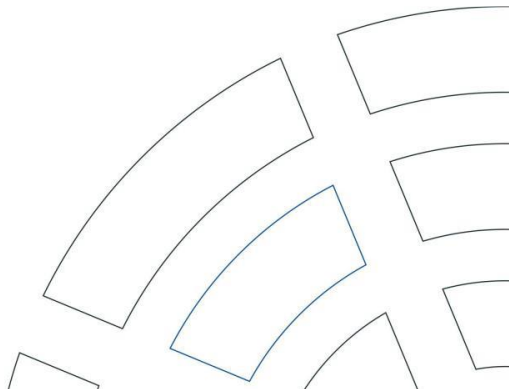
GENERAL REPORT

STRENGTHENING THE PROTECTION OF CRITICAL INFRASTRUCTURE AGAINST CYBER THREATS

General Report
Joëlle GARRIAUD-MAYLAM (France)
General Rapporteur

010 CDS 22 E rev. 1 fin – Original: French – 19 November 2022

Founded in 1955, the NATO Parliamentary Assembly acts as a consultative interparliamentary organisation which is institutionally separate from NATO. This report was adopted by the Committee at the 68th Annual Session of the NATO Parliamentary Assembly. It is based on the information obtained from publicly available sources or from meetings held in the framework of the NATO-PA, which are all unclassified.



EXECUTIVE SUMMARY

Today, the critical infrastructures of NATO Member States and its partners face a rising and unprecedented wave of malicious cyber activities with destabilising and devastating consequences. Public and private entities indispensable to the functioning, well-being and cohesion of Allied societies such as energy providers, telecommunications operators, banks, hospitals, transportation companies and democratic institutions are all being targeted.

The following report highlights that, in spite of an international consensus on the enforceability of international law in cyberspace, the establishment and implementation of standards of conduct in cyberspace remains inadequate. The report also highlights the difficulty in providing cyber protection for crucial allied services in the face of the many different nefarious actors, their objectives as well as the tools and techniques they use. Three case studies illustrate the impact of malicious cyber activities on allied and partner societies and analyse some of the policies and measures adopted to address such attacks.

The scale and magnitude of cyber threats to critical infrastructures calls for Allies to intensify their national and collective responses. This general report aims to contribute to these efforts. It urges NATO and Member States to ensure that the protection of critical infrastructures against malicious cyber activities is at the very core of their approaches to security and resilience. Moreover, this report recommends practical actions to be taken at national, collective and international levels to strengthen the cyber resilience of key allied services. Finally, it urges the Alliance to translate commitments outlined in its new Strategic Concept into concrete measures as soon as possible.

TABLE OF CONTENTS

I- INTRODUCTION

1. The increase in malicious cyber operations against Ukrainian private companies and public services before and during Russia's illegal and unjustified aggression against the country, and the wave of cyber-attacks using ransomware that impacted many critical companies in NATO member states during the COVID-19 pandemic and thereafter have underlined the serious, complex and protean threat to critical infrastructures in cyberspace.

2. Recently, an international consensus simultaneously emerged on the enforceability of international law in cyberspace and on non-binding standards to protect critical infrastructures from cyber-attacks. However, there are still many areas of dispute between States and the application of this legal framework remains inadequate. Emboldened by this absence of unanimity, cooperation and willingness, and exploiting the increasing accessibility and sophisticated nature of hacking tools and techniques, various state and non-state players frequently conduct devastating malicious cyber operations against allied critical infrastructures. Some of these operations are motivated by profit, while others are intended to obtain political or trade secrets, and others still aim at undermining and intimidating NATO member countries and their partners, thereby challenging the very democratic values on which their societies are built.

3. While digitalisation and an ever-increasing interconnection allow societies to innovate and gain in efficiency, they also make them more vulnerable to cyber operations. The line between physical and digital environments is blurring. Consequently, critical infrastructures are extremely tempting targets for the malevolent agents who conduct such operations, as information and communication technologies are now indispensable to their functioning. Yet they represent the backbone of our societies. The well-being, livelihood and stability of our allied populations depend on these technologies. The destruction or degradation of their information networks by a cyber-attack can thus have a considerable human, economic and political cost.

4. Since the 2000s the Allies have progressively been adopting policies and measures to strengthen the resilience of their critical infrastructures to tackle this threat. They have developed innovative and efficient national responses at various levels: strategic and structural, regulatory and operational, and diplomatic and multilateral. While the cyber protection of critical utilities is primarily a national prerogative, NATO also contributes to these efforts to increase cyber protection by promoting the exchange of best practices between Allies and their partners and by reinforcing their cyber defence capacities with practical exercises and training.

5. NATO's new Strategic Concept, which was adopted at the Madrid Summit in June 2022, highlights that "Cyberspace is contested at all times. Malign actors seek to degrade our critical infrastructure, interfere with our government services, extract intelligence, steal intellectual property and impede our military activities." (NATO, 2022a). In the Communiqué of the June 2021 Brussels Summit, the NATO Heads of State and Government had already noted "cyber threats to the security of the Alliance are complex, destructive, coercive, and becoming ever more frequent". They also underlined that "resilience and the ability to detect, prevent, mitigate, and respond to vulnerabilities and intrusions is critical". This report is designed to support efforts to improve the response to cyber threats facing Allied societies. It urges the Member States and NATO to ensure that the protection of critical infrastructures against malicious cyber activities is at the very core of their approaches to security and resilience. In this regard, it underlines the importance of implementing the commitments made in NATO's new Strategic Concept into concrete measures. In particular, it urges the Allies to adopt an integrated, whole-of-society approach to cybersecurity, to intensify their cooperation with each

other and with their partners in fighting cyber threats, and to pursue their commitment to the development of international standards governing cyberspace and their application.

6. Within the scope of this general report, critical infrastructures (or essential services and utilities) are defined as any network, facility or system essential to the well-being, proper functioning and cohesion of a society. This includes public and private actors involved in such key sectors as energy, finance, telecommunications, food and water supply, transportation and medical services. This report also incorporates into this definition the electoral institutions and processes that form the backbone of allied democratic societies.

II- PROTECTING CRITICAL INFRASTRUCTURE AGAINST CYBER THREATS: A NASCENT INTERNATIONAL LEGAL FRAMEWORK WITH A COMPLEX AND INSUFFICIENT IMPLEMENTATION

A. THE GRADUAL RECOGNITION OF THE ENFORCEABILITY OF INTERNATIONAL LAW IN CYBERSPACE BY STATES

7. Until the beginning of the twenty-first century, cyberspace was largely considered a domain without rules differentiating acceptable and unacceptable behaviour and practices (Schmitt, 2020). Since then, a basic international legal framework was defined by the United Nations. In 1998, the General Assembly adopted a resolution (sponsored by Russia!) calling for "the development in the field of information and telecommunications in the context of international security" (Korzak, 2021). In 2004, a Group of Governmental Experts (GGE) was created to define the responsible behaviours that should be adopted by states in cyberspace. However, the international community only started to address the applicability of and compliance with international law in the cyber domain after the cyber-attacks on Estonia in 2007 and Georgia in 2008 (Schmitt, 2020). The GGE (which currently boasts 25 member states) thus confirmed in reports in 2013, 2015 and 2021 that international law applied in cyberspace (Moynihan, 2019). In 2018, the General Assembly formed a second working group (OEWG) with a similar mandate but open to all Member States. While legitimate concerns were raised about Russia and China using the OEWG to reinforce state control over the Internet, the report that the OEWG adopted in March 2021 largely endorses the non-binding standards adopted by the GGE (CFR, 2021).

8. It stems from the work of these two UN bodies that State and non-State actors should not knowingly engage in, support or enable malicious cyber activities against critical infrastructures (GGE, 2021; GTCNL, 2021). The GGE report also urges States to take all appropriate measures to stop any malicious cyber activity originating from their territory and targeting the critical infrastructures of another State (GGE, 2021). Both groups have drawn up non-exhaustive lists of critical infrastructures that should not be targeted by cyber operations, including healthcare, transportation, sanitation, telecommunications, energy and financial services. Contrary to the OEWG, the GGE adds electoral processes to its list (Ciglic, 2021).

9. Based on the work of the GGE and the OEWG, in October 2021 the UN General Assembly adopted a resolution to promote the responsible behaviour of states in their use of information and communication technologies. This resolution reiterates the principles of the non-violent use of information and communication technologies, the need to prevent their misuse for criminal and terrorist purposes and the need to prevent the outbreak of conflicts in cyberspace. The resolution also raises the possibility of developing additional standards in this area, including legally binding obligations (UN General Assembly, 2021).

B. PERSISTENT DISAGREEMENTS POSING A RISK TO THE CYBERSECURITY OF CRITICAL INFRASTRUCTURES

10. While the applicability of international law in cyberspace is now internationally acknowledged, the absence of binding standards leads to uncertainty as to the willingness of some states to accept the unlawfulness of cyber operations against critical infrastructure. In September 2021, UN Secretary-General António Guterres voiced concerns about the risks posed by the shortcomings of the current international system of cyber governance and urged states to adopt stronger measures to deter cyber-malicious acts against civilian infrastructure and defuse tensions in the cyber domain (UN Security Council, 2022).

11. Some crucial questions remain unanswered. For instance, the threshold for the use of force in cyber operations, including those against critical infrastructure, remains unclear. There are disagreements among states as to the classification of a cyber operation that would result in immediate physical consequences, such as death or significant damage, only indirectly (for example, if patients lose their lives due to a power outage in a hospital resulting from a cyber-attack on an electrical installation) or that would incapacitate a critical infrastructure without physically damaging it. This legal gap engenders uncertainty about the conditions under which a nation may employ force in self-defence to respond to a cyber-attack. As such, it also creates a risk that a divergent interpretation of a low-intensity malicious cyber operation could trigger an armed conflict (Schmitt, 2020).

12. The disagreements between states on the definition of an attack in cyberspace have consequences for the enforceability of international humanitarian law (IHL). IHL expressly prohibits “to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population” (Gisel et al., 2021). An international consensus has emerged regarding its enforceability in the case of malicious cyber activities conducted in parallel with conventional military operations. This implies that the principles of humanity, military necessity, proportionality and the distinction between civilian and military objects and persons are applicable in the cyber domain in situations of armed conflict. However, some NATO countries consider that these principles should also govern malicious cyber activities in a conflict that does not involve conventional military operations. Some Allied States consider that, although humanitarian law is only applicable in war situations, these principles should also be applied in cyberspace in peacetime. Russia and China, among others, disagree and remain ambiguous as to the cyber protection of critical infrastructures in both wartime and peacetime (Security Council, 2021; Basu et al., 2021).

13. There are also ongoing disagreements about the legal framework for countering malicious cyber activities by criminal groups, including against allied critical infrastructures. The Council of Europe’s Budapest Convention (on cybercrime) is the main legal instrument covering this area. The Convention sets out the norms and procedures for responding to cybercrime by states that are party to it. For a long time, Moscow has expressed its opposition to this Convention, which it considers as not being consistent with the principles of sovereignty and non-interference (CFR, 2020). Moscow also views this Convention as being obsolete because it was adopted in 2001. But two additional protocols have been added since then, including one in 2021 (CFR, 2020; Council of Europe, 2022). Consequently, since January 2022, Russia has been lobbying to initiate discussions at the United Nations on the development of an international convention on cybercrime, which could be adopted in 2024. There are serious fears that Russia, with the support of other authoritarian states, will use these negotiations to strengthen government control over what citizens put online and to silence its opponents (Brown, 2021). During these negotiations, several States – including Allied States – and a number of civil society organisations appealed to ensure that the regulation of the threat posed by cybercrime should not be at the expense of respect for democratic values and human rights (Human Rights Watch, 2022).

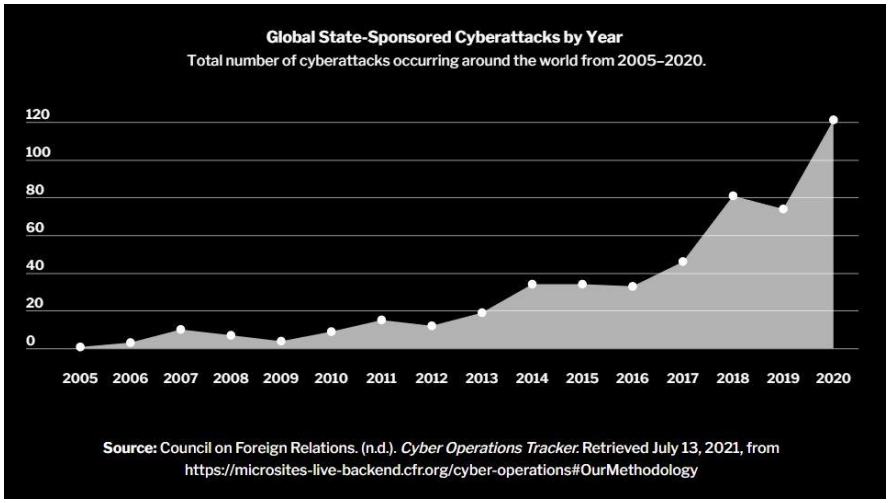
14. The recent surge in ransomware attacks on allied critical infrastructures has highlighted the role played by states that tolerate the presence of cybercriminal groups on their territory, despite their commitments. Many allied countries would like to extend the non-binding rule adopted by the UN working groups on this issue. They want the recognition of a mandatory due diligence rule for cyberspace, whereby states would have a duty to ensure that neither their territory nor their cyber infrastructure is being used to carry out malicious cyber activities. A number of states, including Russia and China, are opposed.

15. Unfortunately, overcoming such divisions at a global scale seems difficult in the short term. But the scope and prevalence of malicious cyber activities against critical infrastructure, particularly Allied infrastructure, leave NATO member states no choice but to further encourage, through dialogue and negotiation, the evolution of an effective and binding legal and regulatory framework to ensure the security of cyberspace.

III- THE DIFFICULTY TO PROTECT ALLIED CRITICAL INFRASTRUCTURES AGAINST MULTIFACETED CYBER THREATS

A. VARIOUS ACTORS WITH DIFFERING OBJECTIVES

16. Numerous actors threaten the cybersecurity of Allied critical infrastructures with very different motives. Among the main perpetrators of such malicious cyber activities are several authoritarian states. Since 2005, the majority of state-sponsored malicious cyber activities worldwide have been conducted by Russia, China, Iran and North Korea (FP Analytics, 2021). Furthermore, the frequency of these malicious cyber activities is increasing. From 2017 to 2020, the number of state-led malicious cyber activities have doubled (Hewlett-Packard, 2021).



17. Russia is the most active in the cyber domain and poses a persistent threat to the critical infrastructures of Allied and partner countries. From July 2020 to June 2021, 58% of malicious cyber activities attributed to a state on a global scale originated from Russia (Burt, 2021). Some of these operations are motivated by political or industrial espionage (FP Analytics, 2021). But most attacks are part of Moscow's strategy of hybrid warfare and the destabilisation of democratic countries. The United States, Ukraine and Germany are the most frequent targets (Burt, 2021). Russia views the cyber domain as part of a broad informational spectrum, spanning from disinformation to electronic warfare. Malicious cyber activities, including those against critical infrastructures, are thereby often mingled with a psychological component (IISS, 2021). They are intended to intimidate target countries, influence their domestic and foreign policies, destabilise their societies by breeding chaos and undermine the trust of citizens in the authorities. For example, this was the intention of the destructive attacks on the Ukrainian electricity grid in December 2015, which were attributed to a Russian cyber military

unit by Ukrainian intelligence services, and which deprived nearly 250,000 people of electricity during several hours (Dupuy et al., 2021; The Economist, 2021).

The multiplication of cyber-attacks against critical infrastructures before and during Russia's new invasion of Ukraine in 2022

Since February 2022, when the Russian armed forces struck Ukraine from the air, land and sea, Moscow has been waging a second, less publicised but equally devastating, cyber assault on the country and its people. The malicious cyber activities, which have been linked by various experts and officials to Kremlin-linked actors, have been launched against critical Ukrainian infrastructure in violation of Russia's pledge to comply with international law in cyberspace (Sanger et al., 2022). These attacks are intended to incapacitate critical services, including government institutions and private companies active in the financial, IT and energy sectors, among others. Moreover, both conventional attacks and malicious cyber activities would seem to be coordinated or at least have common objectives (The Economist, 2022). As a result, these attacks also sometimes affect Allied states.

These malicious cyber activities started just before the Kremlin launched its new brutal, illegal and unjustified assault on Ukraine. In January 2022, a cyber-attack disabled over 70 Ukrainian government websites. Ukrainian authorities blamed the attack on cybercriminals linked to Belarusian intelligence services (The Guardian, 2022; Polityuk, 2022). At the same time, US company Microsoft announced that it had identified wiper software, dubbed *WhisperGate*, in dozens of Ukrainian public and private computer networks, which was designed to disable computer systems while masquerading as ransomware (Microsoft, 2022; Sanger, 2022). The Ukrainian authorities believe that this cyber-attack may also have been carried out by a Belarusian group linked to the Russian authorities (McMillan and Volz, 2022).

One month later, in the days before the onset of the invasion, the websites of several government agencies and two Ukrainian banks were the target of a denial-of-service attack, attributed to Russia by Ukrainian, British and US authorities (Holland and Pearson, 2022). The Ukrainian authorities described the attack as "the largest in the history of Ukraine" (Hopkins, 2022). Additionally, on the eve of the start of the Russian military offensive, Microsoft spotted destructive software that infected hundreds of computers belonging to Ukrainian ministries as well as financial institutions based in Ukraine, Latvia and Lithuania (Bajak, 2022). Within hours, the US company updated its virus detection systems to block the software, dubbed *FoxBlade*, and shared details of its code with several European countries to prevent its propagation (Sanger et al., 2022).

On 24 February, the pace and scale of malicious cyber operations appeared to have escalated further. Approximately one hour before the onset of the invasion, an attack on a US company operating a satellite broadband service disrupted Internet access in Ukraine and in several European countries. According to the British government, this attack was probably aimed at compromising the Ukrainian armed forces by disabling their communication system (Vallance, 2022). Allies have openly condemned this deliberate and malicious cyber activity, which has had a domino effect on Allied countries and have blamed it on Russia.

Since then, malicious cyber operations have escalated. Between December 2021 and March 2022, they doubled every month (The Economist, 2022). In the days leading up to the invasion until the end of April, Microsoft identified 237 cyber operations against Ukraine by actors linked to the Russian state. Approximately 32% of these malicious cyber activities targeted Ukrainian public authorities while another 40% were aimed at operators of critical infrastructure. The US company points out that these actors began pre-positioning themselves to launch these malicious cyber operations as early as March 2021. During the deployment phase of Russian troops along the Ukrainian border, numerous malicious cyber activities were identified as attempts to gain intelligence on Ukraine's military and foreign partnerships. Since the beginning of 2022, the malicious cyber activities have become increasingly damaging and regular, often using destructive software (Burt, 2022). They are now aimed at destabilising Ukrainian society to undermine its ability to resist the invasion. However, the resolve and resilience of the Ukrainian people in the face of the brutality of Russian military aggression demonstrate that they have failed.

With the support of the private sector, Ukrainian authorities and engineers have acquired considerable expertise in tackling these malicious cyber activities effectively and minimising their societal impact. In April 2022, for example, they only narrowly thwarted a malicious cyber activity directed at the country's power grid. If successful, it could have caused power outages for two million people. The software employed in the attempt was similar to that used successfully to disrupt the Kyiv power grid in 2016. However, the authorities have learned from the multiple cyber operations they encountered in recent years and were able to foil the attack (Rundle and Stupp, 2022).

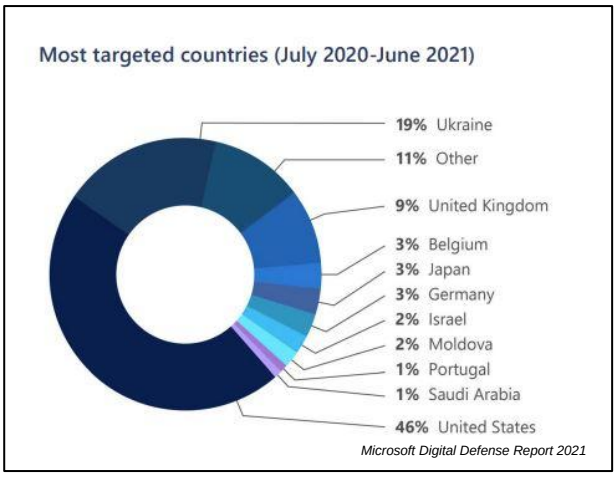
The multiple cyber breaches that have taken place as part of the current invasion have highlighted the importance of cooperation between states and with the private sector. Indeed, the Ukrainian people benefited from the support of the Allies in their response to these assaults. For example, the United States has been helping the country to strengthen its cyber defence for several years. In October and November 2021, the United States deployed soldiers from the US Army Cyber Command to Ukraine to detect Russian malware that could potentially be embedded in the networks of Ukrainian institutions and companies (Srivastava et al., 2022). In addition, Ukrainian authorities also enjoy the support of Allied IT and cybersecurity companies including Cisco, Microsoft and Google. Since malicious cyber activities often target their software, these companies have become increasingly engaged in protecting Ukrainian networks (Srivastava, 2022a).

Cyber-attacks are double-edged weapons. The brutality, unlawfulness and unjustified nature of the Russian invasion and use of cyber-attacks, traced to actors close to the Kremlin, have driven many hackers in Ukraine and around the world to target Russian authorities and companies in retaliation. These attacks are aimed at publishing data, sometimes compromising, or countering Kremlin propaganda by posting anti-war messages on the websites of public institutions or media. Some of the attacks were aimed at critical infrastructures to reduce the capacity of the Russian army to pursue its aggression, without seriously affecting the civilian population. Thus, a cyber operation by a Belarusian dissident group succeeded in slowing down the transportation trains carrying war materials from Russia through Belarus to northern Ukraine in the early days of the invasion (Srivastava, 2022b).

Ukraine's continued resistance, including its cyber resilience, to Russian aggression, the support the country receives from the Alliance, and the military hardships that Russian forces are enduring as a consequence, are all sources of great frustration for the Kremlin. Several Allied governments have expressed concern that this frustration could lead Russian commanders to begin planning larger scale cyber-attacks against Allied companies, particularly against their critical infrastructures (Borger and Farrer, 2022). Preparing effectively for this possibility is paramount. But even if such cyber disruptions should not occur, the use of cyber-attacks before and during armed conflict demands action from the Allies. It is imperative that the Allies should do everything possible to reinforce their response capabilities. The Allies must also step up their political and technical cooperation with their partners. Finally, they should improve the cyber protection of their critical infrastructure, including by increasing the exchange of information and coordination between specialised private companies and the public institutions of Allies and partners.

18. China also poses a threat in cyberspace. Beijing is rapidly expanding its capabilities. In 2015, the country unveiled its ambition to become a major power in this field by 2030 and, to that effect, consolidated and strengthened its armed forces' cyber component (IISS, 2021). China's cyber capabilities are considered the second most sophisticated in the world (FP Analytics, 2021). Malicious cyber activities perpetrated by the Chinese state are primarily aimed at furthering its domestic and external political objectives and conducting industrial and technological espionage against Allied companies and essential utilities.

19. Besides Russia and China, other countries – albeit with more limited capabilities – pose a threat to the cybersecurity of Allied critical infrastructures. One such country is Iran, which has been aggressively building up its cyber capabilities since the *Stuxnet* attack on its own nuclear reactors. The cyber operations launched by the regime are aimed at discrediting democratic processes and institutions in allied countries, stealing intellectual property from companies and sparking unrest and dissension in countries perceived as enemies, most notably in the Middle East but also in the Alliance. Various experts have attributed the cyber-attacks on Israeli water and sewage operators, the US power grid in 2020 and the UK Post Office in 2019 to actors linked to Tehran (Malekos Smith, 2022).

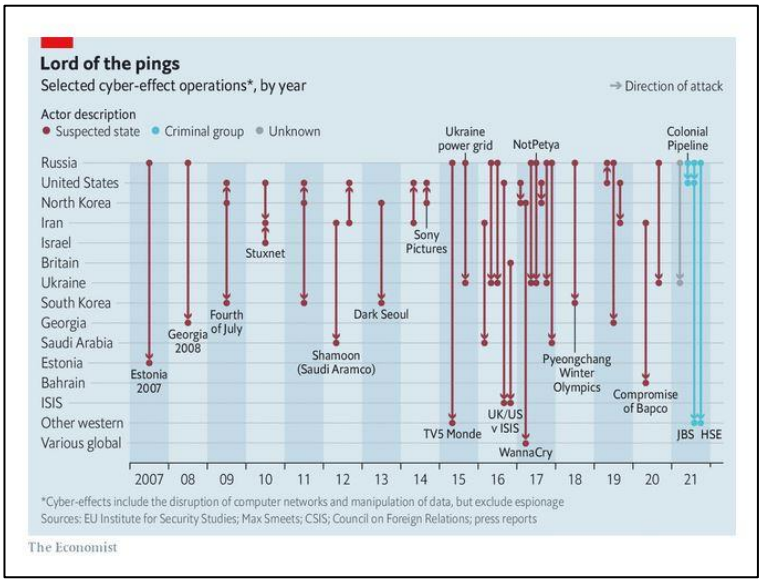


20. Despite having one of the world's lowest Internet presence, North Korea also poses a threat in the cyber area. The authorities allocate considerable resources to the development of their capabilities and conduct malicious cyber operations to steal, defraud and launder money to acquire the financial resources they need to pursue their nuclear programme and ensure the survival of the regime (Sanger and Perlroth, 2020). A recent study estimates that the country may have stolen as much as USD 400 million in digital assets, including crypto currencies, through the use of cyber-malware in 2021 (Chainalysis, 2022a). For its part, in 2019, the UN believed that the country's cyber operations had allowed it to amass a total of around USD 2 billion, which was subsequently allocated to expanding its nuclear programme (BBC, 2022).

21. While cyber operations by states are the most sophisticated and potentially devastating threat to allied critical infrastructures, malicious non-state actors also constitute a challenge in this regard. They are responsible for the bulk of malicious cyber activities worldwide (van der Meer, 2020). These players range from hacktivists (ideologically motivated criminal hackers) to terrorist organisations, malicious insiders (current or former employees who have access to the target's networks) and simple amateurs. Their motivations are manifold. Some seek to build up their reputation, affirm their ideologies or test their skills, while others seek to sow chaos.

22. Yet, the majority of non-state actors attacking critical infrastructure are profit-driven cybercriminals. These individuals or groups exploit the increasing accessibility, simplicity and reproducibility of hacking tools and techniques. Most use ransomware, i.e., malicious software that encrypts the victim's data and is only disabled after the payment of a ransom. This is a growing threat. In 2020, the number of ransomware attacks increased by 485% in comparison to 2019, and ransom payments amounted to more than USD18 billion (Glenny, 2022 Murphy, 2021). While the USA is by far the hardest hit by these attacks, other countries of the Alliance are not spared (Burt, 2021). States where these non-state players are operating, particularly Russia and China, often turn a blind eye to these illegal activities. Indeed, a recent study suggests that 74% of the money looted in ransomware attacks in 2021 went to hackers with links to Russia (Chainalysis, 2022b).

23. Worse still, there are collusions between criminal groups and national authorities. States use IT mercenaries to further their strategic objectives, which enables them to thwart the identification of cyber operations (van der Meer, 2020). Thus, China hires hackers to perform espionage operations across the world. In July 2021 for example, several Allies attributed an infiltration of the Microsoft Exchange platform to a dozen hacker groups backed by the Chinese Ministry of State Security (NATO PA, 2021; White House, 2021). This operation, aimed at retrieving and stealing data, affected tens of thousands of private and public entities and democratic institutions (CCDCOE, 2021b). Other states use cyber mercenaries to exploit the expertise and cyber capabilities they do not possess (Egloff, 2017).

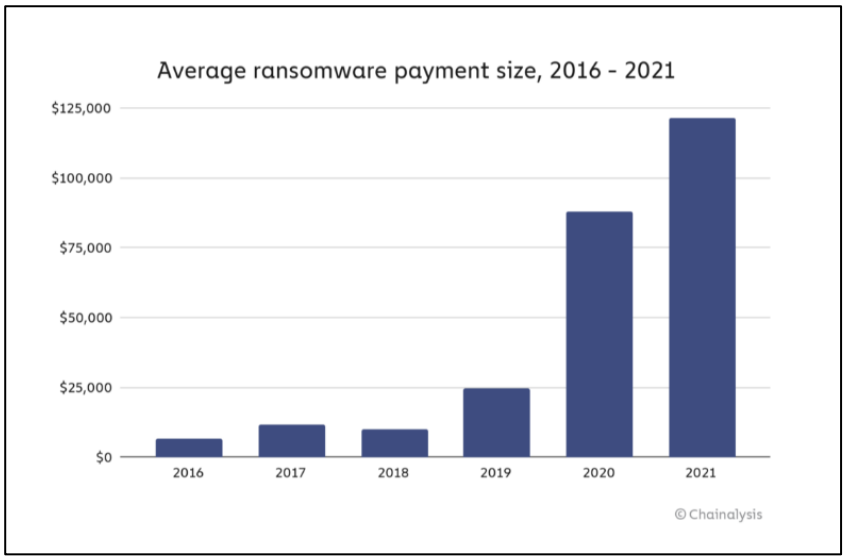


24. The difficulty in fending off cyber threats against allied critical infrastructures is also linked to the wide range of methods used by malevolent actors. In addition to the aforementioned ransomware, malicious actors use a broad arsenal of low-cost, low-traceability techniques, such as phishing, *wipers*, and denial-of-service (DoS) attacks (Monnet, 2021; MEAE, 2022).

B. MULTIPLE AND GROWING THREATS COMPLICATE THE PROTECTION OF CRITICAL SERVICES AND THE DISSUASION OF MALICIOUS CYBER ACTIVITIES

25. The multiplicity of actors, their targets and the techniques used complicates the cyber protection of allied critical infrastructures. Dealing with this multi-faceted threat requires significant investments in cybersecurity. But today, these investments are far too limited, and some organisations still rely on obsolete systems. These vulnerabilities offer easy access points for hostile actors (McCormick and Murphy, 2021). The poor level of cyber security of certain allied critical infrastructures enables hackers to go undetected for lengthy periods of time and thus cause greater damage and disrupt the performance of the infected target when it is at its most vulnerable. Despite these risks, operators are often slow to invest in securing their networks because commercially available tools are both expensive and not subject to common standards for measuring their actual effectiveness (The Economist, 2021).

26. The recent proliferation of malicious cyber activities conducted by non-state actors, particularly through ransomware, has highlighted the necessity for the operators of critical infrastructures to protect their networks more effectively. According to a recent survey, only 31% of private energy companies feel prepared to respond to a cyber-attack on their networks (Siemens, 2021). This lack of preparedness exposes critical infrastructures to cyber risks, and they respond to these threats in a counter-productive manner when they materialise. Often, large companies that fall victim to ransomware attacks prefer to hide the breach and pay the ransom demanded. This allows them to salvage their reputation and avoid the destruction or publication of their data (The Economist, 2021). In turn, this attitude creates a vicious circle that incites malicious actors to repeat the attacks. Another consequence is the rise in ransom payments. On average, these have risen from USD 25,000 in 2019 to USD 118,000 in 2021 (Chainalysis, 2022c).



27. In order to deter malicious cyber activities against critical infrastructures, it is imperative to identify and punish the perpetrators. But the multiplicity and multiplication of cyber threats complicate this attribution. State and non-state attackers sometimes work together on an ad hoc basis or masquerade as one another. Often, they cover their tracks by using covert relays (botnets) or intermediaries (proxies), sometimes in several jurisdictions. While an attacker's objectives may reveal its identity, it is often very difficult to identify and distinguish the perpetrators (Lindsay, 2015). When a malicious cyber activity is identified, the interrelationships binding the criminals increases the difficulty of ascertaining whether it is, for example, financially motivated, economically motivated, politically or ideologically motivated (Slayton, 2017). However, in recent years, NATO countries have been using technological advances to increase their technical abilities to "ascribe", i.e., naming the perpetrators of certain cyber-attacks. They have also forged valuable partnerships in this field with private companies and civil society (FP Analytics, 2021). Beyond the technical aspects, however, the attribution of a cyber-attack remains a political act. Once reluctant, Allies are now increasingly eager to publicise the activities of nefarious actors against their critical infrastructures (Moynihan, 2019). This was the case in July 2021, when several Allies attributed a cyber-attack against the Microsoft Exchange platform to hacker groups linked to the Chinese authorities (Follain et al., 2021). Similarly, as mentioned above, some Allies have publicly attributed a cyber-attack, carried out one hour before the start of its new invasion of Ukraine, against the internet and communications satellites network operated by the American company Viasat to Russian military intelligence (Corera, 2022).

Cybersecurity of critical infrastructures and protection of personal data and privacy

The protection of personal information and the cyber security of critical infrastructures are intimately intertwined. As a consequence of the increasing digitalisation of their processes, critical infrastructures operators increasingly manage or store their users' personal data. It is therefore crucial to ensure a high degree of protection for this data against malicious cyber activities to respect the private lives of citizens. Confidential information cannot be stored on insufficiently protected networks.

In contrast, however, some of the activities and standards designed to reinforce the cybersecurity of users' personal data in critical infrastructures might result in a secondary concern for privacy. For example, the increased vigilance of computer networks to identify potential vulnerabilities and thwart cyber-malware often requires access to – and sometimes the analysis of – vast amounts of personal information.

It is thus essential to find the right balance between providing cybersecurity to the networks of critical infrastructures operators and guaranteeing the respect and protection of the personal data and privacy of citizens. Legislation in this area will have to address these two and sometimes contradictory considerations. Moreover, government regulatory and privacy institutions have an indispensable role to play with ensuring the continued implementation of measures to improve the cybersecurity of critical infrastructure. It is also imperative that relevant national authorities should establish a dialogue with the operators of critical infrastructures, both private and public, to identify common solutions to prevent vulnerabilities and malicious cyber activities that affect personal data. Finally, at an international level, Allies must work to ensure that any efforts to guarantee the security and stability of cyberspace, including the protection of critical infrastructures, do not result in a compromise of democratic values and respect for the rights of citizens to privacy and the protection of personal data.

IV- THE IMPACT OF MALICIOUS CYBER ACTIVITIES ON CRITICAL INFRASTRUCTURES IN ALLIED AND PARTNER COUNTRIES: THREE CASE STUDIES

A. PRIVATE COMPANIES FACING CYBER RISKS: THE 2021 ATTACK ON OIL PIPELINE OPERATOR COLONIAL PIPELINE

28. Most of the critical infrastructures in Allied and Partner countries are now owned and operated by the private sector. This is both a source of efficiency and vulnerability. The aim of essential and non-essential companies is the maximisation of profits, which leads them to become increasingly innovative. However, very often, these companies do not prioritise cybersecurity investments. Their public vitalness also makes them ideal targets for malicious actors. Thus, in recent years, malicious cyber activities against private companies in sectors crucial to the functioning of our societies have proliferated within the Alliance and its partners. State actors also resort to such attacks. As previously reported, since the start of the new, unwarranted and illegal invasion of Ukraine by Russia in February 2022, a spate of cyber-attacks, ascribed to Russia by multiple experts and officials, is targeting private Ukrainian companies, including a number of banks, the post office and the power grid operator.

29. However, most of today's malicious cyber activities are carried out by non-state parties and are often motivated by profit. No sector is left unscathed. For instance, the transport sector was targeted when, in June 2021, a ransomware attack caused disruptions to shipping services in the state of Massachusetts (McMillan et al., 2021). Likewise, such attacks can jeopardise allied food security. Also in June 2021, a group of Russian cybercriminals brought the computer systems of JBS, the world's largest meat processing company, to a standstill for several days, resulting in the closure of most of its plants (Harris and Lee, 2021). The telecommunications industry has not been left unscathed. In August 2021, the details of

50 million customers of T-Mobile, the United States' second largest mobile telephone operator, were successfully stolen by a US hacker (Fitzgerald and McMillan, 2021). However, cyber-attacks against the energy sector pose the highest risk of creating a cascade of disruptions, with potentially catastrophic consequences for Allied resilience. Indeed, all the other sectors rely on energy infrastructures for their operations.

30. In May 2021, the cyber-attack against US company Colonial Pipeline demonstrated the vulnerability of critical companies to malicious cyber activities and their devastating impact on allied societies. Experts have ascribed this attack to the Russian-based cybercriminal group *Darkside*, believed to be tolerated by the Russian government, they successfully hacked into the computer systems of the company, which supplies nearly half of the fuel used on the US East Coast (Bing and Kelly, 2021; Rivero, 2021). The attack forced Colonial Pipeline to interrupt the flow of oil through its pipeline system for six days, which caused severe gasoline shortages and a sharp increase in price. Several airports and airlines were also affected (Johnson, 2021). The company was only able to regain control of its systems and resume operations after paying the cyber criminals more than USD 4 million in ransom (The Economist, 2021).

31. Allies must learn from this attack and the disruption it spawned. First of all, it is necessary to increase pressure on states that harbour cybercriminals on their soil and tolerate their illegal activities in defiance of their international commitments. President Biden said that Russia had "some responsibility for handling" the cyber-attack on the Colonial Pipeline (RFE, 2021). Secondly, this cyber-attack raised the spectre of ransom payments to criminal groups. While US authorities were ultimately able to recover about half of the amount paid by Colonial Pipeline, the payment of ransom emboldens cybercriminals to pursue attacks against critical infrastructures. Thirdly, this cyber-attack emphasised the importance of stronger cooperation between public authorities and the private sector and the necessity to adopt minimum standards for critical businesses in the field of cyber security.

B. CYBER THREATS TO ESSENTIAL PUBLIC SERVICES: THE 2021 CYBER-ATTACK AGAINST THE IRISH HEALTH SERVICE

32. Public services are frequently the target of malicious cyber activities. Indeed, public services represent prime targets for state actors who are intent on destabilising the societies of allied and partner countries. In 2007, for example, Estonia was faced with a coordinated cyber-attack campaign against several critical infrastructures and entities, including government websites. This campaign aimed to sow confusion and chaos in the country after Russia took umbrage at the removal of a Soviet-era statue in Tallinn.

33. Owing to their sometimes-insufficient level of cybersecurity and essential nature, public services are also vulnerable to profit-driven cybercriminals. One of the most vulnerable public services is the health sector. The number of malicious cyber activities in the health sector is steadily escalating both inside the Alliance and beyond. They have a disastrous impact on the lives of citizens and come at a high financial cost. In 2020, ransomware attacks struck more than 400 hospitals in Germany and in the United States, with estimated losses of USD 67 million (FP Analytics, 2021). Cyber-attacks targeting medical facilities in Germany and the Czech Republic, among others, have also been reported in recent years (CCDCOE, 2022) and more recently in France with a ransom demand of USD 10 million – which was reduced to one million after negotiations with the GIGN – urging the country's government to unblock EUR 20 million in addition to the 25 million initially programmed in 2021 and 2022 to reinforce the cybersecurity of health care facilities (Le Figaro, 2022) and provide training for 350 additional negotiators. Similarly, in 2017, around a third of UK National Health Service organisations were brought to a standstill by a cyber-attack linked to the *WannaCry* ransomware (Hern, 2017).

34. The May 2021 cyber-attack on the Irish health service had already illustrated the urgency of strengthening the cyber security of health infrastructures. The hackers (identified by information technology experts as the Russian-based cybercriminal group *Wizard Spider*) blocked access to the health service's data by deploying ransomware (Reynolds, 2021). They then demanded payment of a USD 20 million ransom in exchange for a decryption tool to restore access to the data (BBC, 2021). The Irish government refused to pay the ransom and attempted to mitigate the impact of the cyber-attack on the running of hospitals (Reynolds, 2021). Eventually, given the determination of the authorities, the cybercriminals sent the decryption tool to them without compensation (BBC, 2021). However, it took almost six months for the healthcare system to fully recover from the cyber-attack (Meskill, 2021; Hutton and Bray, 2021).

35. Two major lessons must be learned from these abhorrent cyber-attacks. First of all, the current cybersecurity of public services is inadequate in light of their societal indispensability. Indeed, many essential agencies underestimate the critical importance of cyber security because of conflicting priorities and limited resources. A report investigating the breaches that were exploited in the Irish hacking attack revealed that the Irish health system's level of cyber protection was not proportionate to the size and importance of the service. Since then, the health system has significantly upgraded its response capabilities. For instance, the Irish health system implemented a continuous monitoring service for its IT network (eHealth Ireland, 2022). However, it is essential that the Allied and Partner Public Services grasp the scale of such threats and invest in their cybersecurity ahead of attacks, not only in reaction to them.

36. On the other hand, the Irish authorities, like their French counterparts, demonstrated great courage in refusing to pay the ransom demanded by the cybercriminals. This principled response may have prolonged the duration of the attack and thus worsened its consequences, but it also set a precedent for the most appropriate response to such extortion and thereby deter future malicious cyber activities.

C. THE INTRUSION INTO THE DEMOCRATIC NATIONAL COMMITTEE'S NETWORKS IN 2016 AND THE NECESSITY TO SECURE THE CYBER RESILIENCE OF DEMOCRATIC PROCESSES AND INSTITUTIONS

37. Electoral institutions and processes should be considered critical infrastructures. Indeed, the faith of citizens in a democracy is based on the proper functioning and security of this type of infrastructure. In recent years, several authoritarian states have been accused of launching malicious cyber activities against these democratic states in order to undermine this trust and advance their own authoritarian models. From 2015 to 2018, at least 22 election-related malicious cyber activities hit 16 countries on six continents (NIS Cooperation Group, 2018).

38. In addition to election-related disinformation campaigns (Sanchez, 2021) and surveillance and espionage activities against the opponents of authoritarian regimes (Glowacka et al., 2021), three types of malicious cyber activities can be identified. Firstly, malicious actors sometimes attempt to disrupt the operation of an electronic voting or ballot counting system. In 2014, four days before a parliamentary election in Ukraine, malware was used to mislead the vote-counting system and deliberately tamper with the election result. Fortunately, the software was successfully deleted before the declaration of the outcome, thus preventing it from publishing erroneous results (CCDCOE, 2021c). As Russia becomes increasingly embroiled in its illegal war against Ukraine, there are fears that it could be trying to use cyber-malware to disrupt forthcoming Alliance elections, including the upcoming US mid-term elections in November 2022 (Kagubare, 2022).

39. Secondly, cyber operations were launched against electoral and democratic institutions. Electoral commission websites were targeted, for example in Bulgaria and the Czech Republic (Reuters, 2017a). Parliaments have also been targeted. For example, according to the Norwegian authorities and German intelligence services, Norwegian and German parliamentary networks were infiltrated by hackers linked to China in 2021 and Russia in 2015 respectively (Buli, 2021; BBC, 2016). Electoral records are also being targeted. In 2020, hackers connected to the Iranian regime sent threatening messages to several thousand voters whose contact details were obtained by infiltrating such records in order to influence, unsuccessfully, the 2020 US presidential election (Sanger and Barnes, 2021b).

40. Thirdly, several malicious cyber activities have been directed at political figures. In 2020 and 2021, the personal email inboxes of more than 30 Polish parliamentarians, government officials and journalists were targeted by a cyber operation (Cerulus, 2021). Most of these malicious cyber operations aim at gaining access to a candidate's emails and make them public in the context of an election campaign. In 2017, during the French presidential election campaign, Emmanuel Macron's team was a target of a number of intrusions by hackers (identified by a computer security firm as originating from the *Pawn Storm* group, also known as *Fancy Bear* or *APT28* and linked to the Russian military intelligence service (GRU)) (Reuters, 2017b). In September 2021, the German Foreign Office reported on Russia's role in a hacking campaign aimed at parliamentarians by means of fake emails. The purpose of the campaign was reportedly to obtain confidential information that could be used to destabilise or sway the upcoming election (Cerulus and Klingert, 2021).

41. The similar cyber operation that leaked more than 20,000 internal emails from staffers of the Democratic National Committee and Hillary Clinton's team during the 2016 US presidential campaign has left its mark. Computer hackers sent phishing emails to some members to steal their credentials, access their networks and then extract the emails. These emails were then released to the public in order to sway opinion at a pivotal point in the election campaign (Smith, 2016). According to US intelligence agencies, Russian authorities were behind the cyber operation (ODNI, 2017).

42. Lessons should be learned from these attempts at destabilisation. The Alliance should strengthen the cyber resilience of its democratic institutions and processes. Some countries, such as France, have scrapped their plans for Internet voting due to this potential risk of intrusion. Allied governments should prioritise electoral cyber security in their cyber defence strategies, reinforce the protection of the entities involved, develop deterrence and be prepared to use robust and effective countermeasures as necessary to defend their values in cyberspace.

V- THE APPROACH OF THE ALLIANCE TO PROTECT CRITICAL INFRASTRUCTURES FROM CYBER THREATS

A. MEASURES UNDERTAKEN BY MEMBER STATES

43. Essentially, building and maintaining the cyber resilience of critical infrastructures against malicious cyber activities remain a national responsibility of States. When faced with the rising number of this type of operations, the Allies have responded in three ways: strategic and structural, regulatory and capability-based and finally, diplomatic and multilateral. Since it is not possible to analyse the individual responses of all 30 Allies, this report highlights specific national policies and innovative initiatives that, if replicated across the Alliance, would strengthen its collective resilience.

44. Allied countries have been developing national strategic and structural frameworks to offer greater protection to their societies and critical infrastructures against malicious cyber activities. One such example is Estonia, as our Committee observed during a virtual visit in April 2021 (NATO PA, April 2021). Indeed, the Estonian society is one of the world's most digitalised. This mainstreaming of the cyber domain into everyday life is both a catalyst for economic growth and administrative efficiency, as well as a source of vulnerability, as evidenced by the aforementioned cyber-attack campaign of 2007 which disabled several critical infrastructures simultaneously. This attack prompted Estonia to reinforce its domestic cyber resilience. The following year, the country adopted its first national cyber security strategy, which has since been updated several times. One of the cornerstones of this strategy is the protection of the country's critical infrastructure and the uninterrupted availability of essential services. To this end, the Estonian government has created a secure information and data sharing architecture based on electronic identity cards and the X-Road system, ensuring interoperability between different essential services while guaranteeing segmentation of access to sensitive data (NATO PA, 2021).

45. In 2021, a hacker took advantage of a breach in the data-sharing system to download some 300,000 identity photographs used by the Estonian police and customs authorities. However, the compartmentalised approach of the network prevented the hacker from accessing the database of identity documents. In reaction to this attack, the Estonian authorities introduced a national bug bounty programme whereby hackers uncovering vulnerabilities in state IT systems can collect a reward if they notify the authorities (Information System Authority, 2022).

46. Estonia has also introduced measures to ensure the uninterrupted operation of critical infrastructures in the event of a malicious cyber operation on one or more of them by strengthening the availability of alternative solutions. Surveillance, analysis and reporting systems are also being developed at several levels to improve the sharing of information concerning potential or ongoing cyber-attack between different public and private operators in order to more effectively thwart them (Ministry of the Economy of Estonia, 2022).

47. Allied States are also taking regulatory and capability measures to strengthen the protection of their critical infrastructures. Responding to the cyber-attack on the Colonial Pipeline, President Biden issued an executive order imposing minimum strict cybersecurity standards for software sold to the US government (Sanger and Barnes, 2021a). In addition, the United States has initiated several initiatives to increase cyber security in the private sector. These efforts are all the more critical given that 85% of federal critical infrastructures are privately owned (FP Analytics, 2021). Specifically, the US government has launched a large-scale initiative to improve the cybersecurity of the companies operating critical infrastructures.

48. While the Colonial Pipeline attack showed the limits of the US authorities' previously preferred collaborative approach to the cybersecurity of critical enterprises, the US authorities introduced for the first time an obligation for these companies to inform the relevant authorities within 72 hours in the event that they fall victim to a malicious cyber operation. This new obligation should allow for improved information sharing between the operators and the authorities and, therefore, a more effective response capacity. In addition, companies are obliged to alert the authorities within 24 hours if they are paying ransom to cybercriminals (Conger, 2022). The Czech Republic gives another example of good practice. To strengthen the capacity of its core businesses to tackle cyber threats, the country has introduced exercises and drills involving every sector of its economy. These exercises are designed to identify the vulnerabilities of each company and help to address them (Warrell, 2021).

49. Other multi-sector initiatives emerge in some Allied countries. For example, in Denmark, the Consumer Council, non-profit organisation TrygFonden, financial entities and the (Danish)

Crime Prevention Council have joined forces to develop a cybersecurity application for the general public. This application offers up-to-date information on digital scams, viruses and malware. It also enables banks and relevant public services to issue real-time security warnings. Such initiatives should be encouraged and replicated in other Member States (Venkina, 2021).

50. On the international level, Allies foster the implementation of cyberspace security standards. They cooperate with partner states to punish cyber criminals found guilty of malicious cyber activities against allied entities, including critical infrastructures. For example, in June 2021, the US authorities worked with their South Korean and Ukrainian counterparts and Interpol to arrest and charge members of the Ukraine-based hacker group *Cl0p* (Murphy, 2021). Additionally, several allied countries recently increased their pressure on states – including Russia – for failing to address criminal activities of groups they harbour. During the meeting with his Russian counterpart in June 2021, President Biden warned that Russia would face a US response if it continued to condone cybercriminal groups conducting cyber operations against allied critical infrastructure on its territory (Barotte, 2021; Nakashima and Scott, 2021).

51. Moreover, the Allies are working to strengthen the legal framework governing the behaviour of states and the protection of critical infrastructures in cyberspace. In this area, France is actively involved. It champions the protection of a secure, stable and open cyberspace in its negotiations within multilateral organisations, including the UN, the G7 and the Organization for Security and Co-operation in Europe – OSCE (MEAE, 2022). The active role that the country plays in cyber diplomacy initiatives was illustrated by the successful introduction of the Paris Call for Trust and Security in Cyberspace in 2018. This initiative allowed for the creation of a forum for reflection on responsible behaviour in cyberspace that includes states, the private sector, the research community and civil society. This reflection is structured around nine principles, the first of which is to "Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure." (Paris Call, 2022) The Paris Call has been endorsed by more than 1,200 entities, including states, private companies, public institutions and civil society representatives. Its inclusive nature mirrors the belief among Allies that the elaboration of comprehensive, effective, and enforceable standards demands the involvement and support of all societal actors.

B. NATO'S ROLE IN BUILDING CYBER SECURITY AND RESILIENCE

52. The task of building cyber protection for critical infrastructures is a domestic responsibility. However, a breach in the operations of critical infrastructures in one Allied country can impact the resilience and the security of the Alliance as a whole. The resilience and cyber security of critical infrastructures are therefore two indissociable areas that must be developed collectively.

53. NATO's new Strategic Concept, adopted in June 2022 at the Madrid Summit, acknowledges the importance of Allied efforts in this area. It specifically underlines the fact that "Maintaining secure use of and unfettered access to space and cyberspace are key to effective deterrence and defence." It also indicates the Allies' commitment to "improve our ability to operate effectively in space and cyberspace to prevent, detect, counter and respond to the full spectrum of threats, using all available tools" and to work "a more robust, integrated and coherent approach to building national and Alliance-wide resilience against military and non-military threats and challenges to our security", including cyber threats (NATO, 2022a). It is imperative that NATO should now translate these commitments into concrete measures and policies. In doing so, NATO will be able to use previous efforts in this area.

54. Indeed, over the past two decades, NATO has already elaborated a comprehensive cybersecurity policy. As early as 2002, it placed cyber defence on its agenda. In 2008, following the 2007 malicious cyber activities against Estonia, NATO adopted its first cyber defence policy, which paved the way for many subsequent advances. In 2014, Allies explicitly stated that a cyber-attack could trigger the invocation of Article 5. If necessary and on a case-by-case basis, Heads of States and Governments reserve the right to respond, not necessarily limited to the area of cyberspace, to cyber-attacks targeting an Ally. In 2016, the Heads of State and Government adopted a *Commitment on Cybersecurity* recognising cyberspace as an operating environment and stressing the need to strengthen national cyber defence capabilities. This Commitment places a priority on improving the cyber defence capabilities of national infrastructures and networks. In February 2019, NATO established a strategic response options handbook to address malicious cyber activities. Finally, at the Brussels Summit in 2021, the Allies endorsed a Comprehensive Cyber Defence Policy with an Action Plan approved by the Heads of State and Government at the Madrid Summit in 2022.

55. Concurrently and jointly, NATO has been developing its approach to resilience under Article 3 of the North Atlantic Treaty. In 2016, the NATO Heads of State and Government adopted a *Commitment to Enhance Resilience*. They note that "these challenges require Allies to maintain and protect critical civilian capabilities", and that they will strengthen and enhance "as a matter of priority, the protection of our national infrastructure and networks against the increasing threat and sophistication of cyber-attacks." At the same summit, they identified seven core resilience criteria to measure and guide national resilience efforts. These criteria (which have been updated several times since 2016) include: continuity of government and essential public services, energy supplies, uncontrolled movement of people, food and water resources, telecommunications (including 5G networks) and cyber networks and transportation and health systems. In 2021, at the Brussels Summit, the Allies adopted a *Strengthened Resilience Commitment* in which they listed "malicious cyber activities" as one of the "threats and challenges to our resilience, from both state and non-state actors". They are committed "to ensure the resilience of our critical infrastructure (on land, at sea, in space and in cyberspace) and key industries."

56. Together with the enhancement of its resilience and cyber defence policies, NATO has also established institutions involved in strengthening coordination and information exchange on cyber threats with and among member states, developing a common approach to cyber defence capability building among Allies, and elaborating common procedures for dealing with crisis situations. As we witnessed when our Committee visited The Hague in May 2022, the NATO Communications and Information Agency offers specialised services to NATO and Allies in order to prevent, detect, address and recover from cyber security incidents. Through its Computer Incident Response Capability (NCIRC), whose primary role is the protection of the organisation's networks, it also regularly shares its analysis of cyber threats with the Allies.

57. Additionally, a Cyber Operations Centre integrated into NATO's strengthened Command Structure is due to be operational in 2023 with the aim of enabling NATO to better analyse and coordinate its operational activities. The Cyber Defence Committee provides a forum for Allies to exchange views at the political level on malicious cyber activities, targeting them and discussing possible joint responses, to elaborate the Alliance's strategy in this constantly competitive area and to share intelligence on threats in cyberspace. Furthermore, the committee for resilience brings together military and civilian experts (including representatives from national governments and the industry) to develop common policies to address emergency situations, such as a cyber-attack on critical infrastructure. It also provides governments with cybersecurity experts and serves as a forum for member states to share experiences and best practices, particularly regarding the resilience of critical infrastructures. Finally, in May 2022, the North Atlantic Council met for the first time with senior cyber

coordinators to review the cyber consequences of the Russian invasion of Ukraine and the progress achieved by the Allies in developing their cyber defence capabilities (NATO, 2022b).

58. NATO also organises cyber defence training and exercises to help enhance national capabilities, including in the area of cyber protection of critical infrastructures. NATO's Oberammergau school in southern Germany and its NCI (Communications and Information Academy) in Oeiras, Portugal provide training in this field for the staff of member and partner countries. The Allied Command Transformation organises the *Cyber Coalition* exercise, NATO's largest annual cyber defence exercise. These exercises are designed to test and enhance the individual and collective cyber operational capabilities of Allies, including in the face of a cyber-attack on critical infrastructures. For example, the *Cyber Coalition* 2021 exercise scenario included malicious cyber activities against Allied gas supply pipelines and vaccination programmes (SHAPE, 2021).

59. Acknowledging that cyber threats do not respect borders and that tackling them requires the involvement of all relevant actors, NATO has developed a wide range of cooperation efforts in the field of cyber security. It works with the Partner States through its defence capacity-building assistance, the DCB Trust Fund and the Science for Peace and Security (SPS) Programme (NATO, 2019; NATO, 2021). In addition, since 2016, NATO has established strengthened cooperation with the EU in the fight against hybrid threats. Cyber defence is one of the principal areas of focus. In February 2016, the two organisations signed a Technical Arrangement on Cyber Defence aimed at strengthening their joint efforts to better prevent, detect and respond to malicious cyber activities (NATO, 2016). The two organisations exchange information and best practices and engage in each other's training, research and exercises. Finally, NATO recognises that the expertise and involvement of the private sector are essential in the fight against cyber threats. Therefore, in 2014, it set up a NATO-Industry Cyber Partnership (NICP) to facilitate information sharing with representatives of the private sector and national cyber warning and response centres. It also involves them in its exercises, training and education.

60. Based in Tallinn, Estonia, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE, not an integrated part of NATO but accredited by NATO) helps define and develop the international legal framework for behaviour in cyberspace. In 2013 and 2017, it brought together international policy and legal experts to draft the so-called "Tallinn Manual", which sets out standards for international law applicable to cyber warfare, including the protection of critical infrastructure. In 2021, the CCDCOE initiated a five-year project to update the manual. The CCDCOE also organises annual training and exercises, including the *Locked Shields* and *Crossed Swords* exercises. The scenario of these exercises regularly includes malicious cyber activities against critical infrastructures. For example, the *Locked Shields* 2021 exercise focused on the protection of electricity and water supply services. The 2022 exercise scenario also comprised the protection of various critical infrastructures, including an electricity grid, a water purification facility, a satellite communications system, financial institutions and 5G facilities (NPR, 2022). Finally, the CCDCOE acts as a forum for cooperation between states. Several partner countries contribute to this forum and share their expertise, experience and best practices with the Allied States that are members.

VI- PRELIMINARY CONCLUSIONS AND RECOMMENDATIONS

61. Although they are widely recognised as illegitimate under international law, malicious cyber activities on critical infrastructures keep on increasing within the Alliance and beyond. The recent examples analysed in this report highlight the destabilising and devastating impact that this complex and multifaceted threat can have on the societies of our allies and partners. While the Allies have already responded individually and collectively, further action is urgently needed. This report is designed to contribute to that effort by outlining suggested courses of action for Allied governments and parliaments and where appropriate, NATO bodies at the national, collective, and international levels.

A. AT NATIONAL LEVEL: STRENGTHENING THE PROTECTION OF CRITICAL INFRASTRUCTURES AND ADOPTING AN INTEGRATED AND COMPREHENSIVE APPROACH TO CYBER SECURITY

- *Promote awareness among all stakeholders in society of the importance of their individual roles in the cyber resilience of Allied critical infrastructures:*
  - The Allies should increase their communication *vis-à-vis* essential public and private bodies to promote greater awareness of the seriousness of cyber risks they face and the importance of enhancing and investing in their ability to prevent, repel and overcome a cyber-attack.
  - The contribution of private cybersecurity firms to the efforts in securing cyberspace should be increased. These firms have the ability to quickly identify cyber threats on their networks and act effectively to counter them. Allied and partner governments should therefore enhance cooperation with these firms, notably by creating permanent arrangements for a better exchange of information.
  - Allies should work to educate citizens about the importance of cyber hygiene (i.e., the basic technical measures they should take to ensure the security of information systems they use). These efforts could be implemented through training programmes in schools, businesses and key public services.

- *Develop clear and effective national standards for cybersecurity of critical infrastructures:*
  - Together with all critical sectors, Allies should adopt and enforce robust national laws and high threshold standards for the cyber security of critical infrastructures. It is crucial that these laws and standards should recognise and facilitate the protection of personal data and the privacy of citizens.
  - Following the recent example set by the United States in this area, Allies should introduce minimum standards for software and other cyber security solutions used by public utilities. The introduction of minimum standards could reduce the market viability of non-standard products and allow all major societal actors, including those in the private sector, to benefit from high-quality cybersecurity solutions.
  - Allies should compel the operators of critical infrastructures, including private companies, to share relevant information on malicious cyber activities affecting them as soon as possible with the relevant authorities to subsequently provide timely warning to other operators and thereby help thwart similar threats. The standards adopted in the United States in the wake of the cyber-attack on Colonial Pipeline could serve as an example. Indeed, it is essential that these standards should be uniform amongst the Allies to maximise effectiveness and limit their impact on businesses.

- *Implement practical and effective measures to enhance cyber protection and resilience of critical infrastructures:*
  - Allies should invest more financial and human resources to detect malicious cyber activities against their critical infrastructures. They should also invest in setting up early warning systems to facilitate the exchange of information with operators about

identified threats and methods of responding to threats. It is also crucial to continue and expand research in the field of cyber resilience. Within this framework, Allies should, inter alia, adopt concrete measures to address the current gender gap in the cyber defence community.

- They should conduct regular in-depth network analyses of critical infrastructures with the aim of identifying and addressing potential vulnerabilities ahead of cyber-attacks. Drills and simulations in each economic sector would help identify and eliminate vulnerabilities, in line with the example of the Czech Republic.
- Allied governments should also support investments in cyber defence made by private companies and key public services, particularly for the replacement of old and vulnerable IT systems and reinforce the protection of personal data. In the same way, investments should be made to enhance the cyber security of democratic institutions and processes.
- Allies should oblige the operators of critical infrastructures, both public and private, to develop contingency plans for different types of potential malicious cyber operations.
- Governments should ensure the uninterrupted provision of essential societal services and avoid cascading disruptions within and between sectors in the event that a cyber-attack disables critical infrastructures. To do so, it is crucial to develop business continuity plans in collaboration with the operators. In the same way, contingency plans should be put in place in the event of a failure of electoral systems.
- Governments should strengthen their capacity to communicate swiftly and effectively with the public in the event of a serious cyber-attack to reassure the population and clearly explain measures being enacted in response. These efforts could benefit from an exchange of experiences and best practices, particularly with countries that have experienced or are currently facing attacks, such as Estonia and Ukraine.
- Allied governments might consider emulating Estonia's approach by creating programmes rewarding people for reporting breaches in their systems to authorities, rather than exploiting or releasing them. Some other examples worth replicating include the bug bounty schemes set up in France by the *Agence nationale de la sécurité des systèmes d'information* (ANSSI) to improve the effectiveness of the StopCovid application in May 2020 and by the French Ministry of Defence to strengthen the security of its websites and web applications.

B. AT COLLECTIVE LEVEL: DEVELOPING SHARED RESPONSES TO CYBER CHALLENGES AMONGST ALLIES AND WITH THEIR PARTNERS

- *Place the cyber protection of critical infrastructures at the core of resilience and cyber defence efforts and consolidate allied doctrine on responding to malicious cyber activities against them:*
  - The NATO Heads of State and Government have highlighted the role of tackling cyber threats for the security of the Alliance in the new Strategic Concept. Now it is crucial that the Alliance should translate these commitments into concrete and tangible policies and initiatives.
  - Allies should also expedite the implementation of previously agreed common policies, including the 2016 Cyber Defence Commitment and the Comprehensive Cyber Defence Policy adopted at the Brussels Summit in 2021.
  - They should strengthen the harmonisation and complementarity of resilience and cyber defence policies. Specifically, the national resilience baseline requirements should be reconsidered in light of the current wave of malicious cyber activities on allied critical infrastructures with a view to incorporating the need to strengthen cyber protection.
  - Allies should regularly reiterate that a cyber-attack, particularly against critical infrastructures, may be considered an armed attack warranting a military response under Article 5 of the Washington Treaty as they have reaffirmed in NATO's new

Strategic Concept. In order to discourage such attacks credibly, the Alliance must also be as transparent as possible about the extent of its cyber capabilities.

- Allies should not set a specific threshold at which a cyber-attack would be considered an armed attack. Nor should they specify the exact nature of their collective response to a cyber-attack above that threshold. However, they should continue to reflect on possible joint responses to cyber-attacks below this threshold as necessary to deter the use of such attacks by nefarious State and non-State actors.
- The Allies must also reinforce their advanced defence capability against cyber-attacks by relentlessly observing, prosecuting and neutralising attacks and by making sure that their perpetrators are not spared. This proactive approach is the only effective means of disrupting and defeating the cyber campaigns of adversaries.

- *Reinforce the operationalisation of Allied policies:*
  - Working in collaboration with the European Programme for Critical Infrastructure Protection (EPCIP), Allies should improve the sharing of intelligence on malicious cyber activities against critical infrastructure between themselves and with their partners in order to both facilitate the identification of cyber-attacks and enable other Member States to counter them more effectively.
  - NATO Allies should enhance their individual and collective ability to attribute malicious cyber activities against their critical infrastructure accurately and confidently. In order to better discourage such threats, NATO governments should also display their resolve to name perpetrators proactively and jointly and to punish them through joint sanctions and other retaliatory measures. Allies should also continue to publicly name and, where necessary, punish those states tolerating the presence of criminal groups responsible for malicious cyber activities against critical infrastructure on their territory.
  - While NATO has already set up a number of quick response teams of cyber defence experts capable of assisting a member state that has been the victim of a cyber-attack rapidly, Allies should deploy additional and greater resources to meet requests for assistance from member states whose critical infrastructure is targeted.
  - Allies should build a joint approach to the scourge of ransomware cyber-attacks. To diminish the profitability and attractiveness of these attacks for cyber criminals, Allies should follow the example of Ireland and refuse to pay any ransom when their public services are being attacked. Similarly, critical private companies should be forbidden from paying ransom or should be compelled to publicise any such payments. Alternatively, Allies could emulate the US decision to force any company paying ransom to cybercriminals to notify the relevant authorities within 24 hours.

- *Strengthen the collective resilience of critical infrastructures ahead of cyber-attacks:*
  - Allies should share the information they have on cyber vulnerabilities of their critical infrastructures and the resources deployed to address such vulnerabilities with other Member States. Indeed, critical infrastructures are prone to be affected by disruptions due to cross-border interconnections and should be prepared. They may also share similar vulnerabilities and other Allies could therefore benefit from information on how to eliminate them.
  - NATO institutions should reinforce their role as platforms for exchanging best practices on cyber protection of critical infrastructures between Allies and their partners. The contribution of NATO's Cooperative Cyber Defence Centre of Excellence to these efforts should also be increased.
  - Allies and NATO should expand the integration of malicious cyber activities against critical infrastructures into their cyber exercise scenarios. They should also reinforce the participation of representatives of public and private critical service operators to ensure that their input is better incorporated into responses to cyber-attacks.

- *Increase cooperation with NATO partners:*
  - Allies should increase the sharing of information, experience and best practices with partner countries that have acquired specific expertise in the cyber protection of critical infrastructures. It is particularly important to continue providing full support to Ukrainian authorities in their fight against the repeated cyber-attacks on the country in the context of the new Russian invasion.
  - NATO should intensify collaboration with other international organisations – such as the G7 and OSCE – that are working on cyber security, including that of critical infrastructures. It is of utmost importance to continue building relations with the EU in this area, both at leadership and staff levels.
  - NATO should strengthen, or where necessary create forums for reflection, discussion and cooperation with all major societal actors. More specifically, the role of the NATO-Industry Cyber Partnership should be enhanced to foster the exchange of information and best practices.

C. AT INTERNATIONAL LEVEL: WORKING TO STRENGTHEN THE LEGAL FRAMEWORK AND ITS IMPLEMENTATION

- Allies should coordinate their positions and be united in diplomatic and multilateral efforts to reaffirm, clarify and expand the legal framework governing the applicability of international law in cyberspace and, in particular, the protection of critical infrastructures from malicious cyber activities. They should also encourage the implementation of mechanisms to improve the practical application of international law. They should remain vigilant to ascertain that the tightening of standards for protecting critical infrastructure against malicious cyber activities is not coupled with a loss of democratic values and the respect of citizens' right to privacy and personal data protection.
- NATO Member States should strive to establish, as much as possible, common positions with their partners to exert maximum influence in multilateral negotiations on these issues.
- Allies should also encourage the participation of non-state societal actors playing a central role in cybersecurity in multilateral negotiations. This type of participation would ensure that the perspectives and concerns of the private sector, public institutions, civil society as well as citizens are adequately reflected in the discussions on the standards applicable to cyberspace. The creation of a United Nations Cybersecurity Agenda for Action, as proposed by several Allied States, would enable the implementation of this type of participatory format.

BIBLIOGRAPHY

Appel de Paris, *Les 9 principes*, 2022.

Bajak, Frank, *Cyberattacks accompany Russian military assault on Ukraine*, AP News, 24 February 2022.

Barotte, Nicolas, *La cyberguerre à l'aube d'une nouvelle ère*, Le Figaro, 30 July 2021.

Basu, Arindrajit, Poetranto, Irene and Lau, Justin, *The UN Struggles to Make Progress on Securing Cyberspace*, Carnegie Endowment for International Peace, 19 May 2021.

BBC, *North Korea: Missile programme funded through stolen crypto, UN report says*, 6 February 2022.

BBC, *Irish cyber-attack: Hackers bail out Irish health service for free*, 21 May 2021.

BBC, *Russia 'was behind German parliament hack'*, 13 May 2016.

Bing, Christopher, Kelly, Stephanie, *Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed*, Reuters, 8 May 2021.

Borger, Julian et Farrer, Martin, West warns of Russian cyber-attacks as concerns rise over Putin's nuclear rhetoric, The Guardian, 21 April 2022.

Brown, Deborah, *Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights*, Human Rights Watch, 13 August 2021.

Buli, Nora, *Norway says cyber attack on parliament carried out from China*, Reuters, 19 July 2021.

Burt, Tom, *Russian cyberattacks pose greater risk to governments and other insights from our annual report*, Microsoft, 7 October 2021.

Burt, Tom, *The hybrid war in Ukraine*, Microsoft, 27 April 2022.

Cerulus, Laurens, *Polish politicians hit by 'large-scale' cyberattack, Russia blamed*, Politico, 18 June 2021.

Cerulus, Laurens et Klingert, Liv, *Russia's'Ghostwriter' hacker group takes aim at German election*, Politico, 21 September 2021.

Chainalysis, *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*, 13 January 2022a.

Chainalysis, *Russian Cybercriminals Drive Significant Ransomware and Cryptocurrency-based Money Laundering Activity,* 14 February 2022b.

Chainalysis, *As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict*, 10 February 2022c.

Ciglic, Kaja, *The next chapter of cyber diplomacy at the United Nations beckons*, Microsoft, 30 August 2021.

Conger, Kate, *With Eye to Russia, Biden Administration Asks Companies to Report Cyberattacks*, 23 March 2022.

Council of Europe*, Future of the convention*, 2022.

United Nations Security Council, *The Security Council and Cyber Threats, an Update*, 31 January 2022.

Corera, Gordon, *Russia hacked Ukrainian satellite communications, officials believe*, BBC News, 25 March 2022.

Council on Foreign Relations (CFR), *A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet*, 13 January 2020.

Council on Foreign Relations (CFR), *Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?*, 18 March 2021.

Dupuy, Arnold, Nussbaum, Dan, Butrimas, Vytautas and Granitsas, Alkman, *Energy security in the era of hybrid warfare*, NATO Review, 13 January 2021.

Egloff, Florian, *Cybersecurity and the Age of Privateering*, Carnegie Endowment for International Peace, 16 October 2017.

eHealth Ireland, *After the Cyber Attack is Over*, 2022.

FitzGerald, Drew and McMillan, Robert, *T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their Security Is Awful'*, The Wall Street Journal, 27 August 2021.

Follain, John, Leonard, Jenny and Mehrotra, Kartikay, *U.S., U.K., Allies Tie Chinese Government to Microsoft Hack*, Bloomberg, 19 July 2021.
FP Analytics, *Conflict in the Cyber Age*, 2021.
Gisel, Laurent, Rodenhäuser, Tilman and Dörmann, Knut, *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, International Review of the Red Cross, March 2021.
Glenny, Misha, *The Colonial Pipeline cyber attack is a warning of worse to come*, Financial Times, 14 May 2022.
Glowacka, Dorota, Youngs, Richard, Pintea, Adela and Wolosik, Ewelina, *Digital technologies as a means of repression and social control*, European Parliament, April 2021.
Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE), *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, 14 July 2021.
NIS Cooperation Group, *Compendium on Cyber Security of Election Technology*, July 2018.
GTCNL (*Open-ended working group on developments in the field of information and telecommunications in the context of international security)*, *Final Substantive Report*, 10 March 2021.
Harris, Bryan and Lee, Dave, *Hacking American beef: the relentless rise of ransomware*, Financial Times, 4 June 2021.
Hern, Alex, *NHS could have avoided WannaCry hack with 'basic IT security', says report*, The Guardian, 27 October 2017.
Hewlett-Packard (HP), *New study highlights 100% rise in nation state cyberattacks in last three years*, 8 April 2021.
Holland, Steve and Pearson, James, *US, UK: Russia responsible for cyberattack against Ukrainian banks*, Reuters, 18 February 2022.
Hopkins, Valerie, *A hack of the Defense Ministry, army and state banks was the largest of its kind in Ukraine's history*, The New York Times, 15 February 2022.
Human Rights Watch, *Opening Stages in UN Cybercrime Treaty Talks Reflect Human Rights Risks*, 28 April 2022.
Hutton, Brian and Bray, Jennifer, *HSE may be impacted for six months by cyberattack, says Reid*, The Irish Times, 16 June 2021.
IISS, *Cyber Capabilities and National Power: A Net Assessment*, 28 June 2021.
Information System Authority, *Estonia, Cyber Security in Estonia,* 2022.
Johnson, Jeh Charles, *Cyberattacks on our energy infrastructure: The need for a national response to a national security threat*, Atlantic Council, 13 December 2021.
Kagubare, Ines, *Midterms raise fears of Russian cyberattacks*, The Hill, 14 April 2022.
Korzak, Elaine, *Russia's Cyber Policy Efforts in the United Nations*, Tallinn Papers, 2021.
Le Figaro, *Cyberattaque contre un hôpital en Essonne: les urgences à mi-régime*, 2 September 2022.
Lindsay, Jon, *Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack*, Journal of cybersecurity, Oxford academic, 28 November 2015.
Malekos Smith, Zhanna, *Emerging Cyber Threats: No State Is an Island in Cyberspace*, Center for Strategic and International Studies, 23 March 2022.
McCormick, Myles and Murphy, Hannah, *Hackers target US infrastructure after digitisation on the cheap*, Financial Times, 21 May 2021.
McMillan, Robert and Volz, Dustin, *Ukraine Hacks Signal Broad Risks of Cyberwar Even as Limited Scope Confounds Experts*, The Wall Street Journal, 20 January 2022.
McMillan, Robert, De Avila, Joseph and Bunge, Jacob, *NYC's Subway Operator and Martha's Vineyard Ferry Latest to Report Cyberattacks*, The Wall Street Journal, 2 June 2022.
Meskill, Tommy, *Three quarters of HSE IT servers decrypted*, RTE, 23 June 2021.
Microsoft, *Destructive malware targeting Ukrainian organizations*, 15 January 2022.
Microsoft, *Digital Defense Report*, 2021.
Ministry of Europe and Foreign Affairs (MEAE), *France and Cyber security*, January 2022.
Ministry of Foreign Affairs of Estonia, Cyber security, 2022.

Monnet, Bertrand, *Cybercriminalité : la quête de la « faille »*, Le Monde, 22 August 2021.
Moynihan, Harriet, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, Chatham House, December 2019.
Murphy, Hannah, *Ukraine arrests ransomware gang in global cyber criminal crackdown*, Financial Times, 16 June 2021.
Murphy, Hannah, *'It's a battle, it's warfare': experts seek to defeat ransomware attackers*, Financial Times, 14 May 2022.
Nakashima, Ellen and Scott, Eugene, *Biden tells Putin the U.S. will take 'any necessary action' after latest ransomware attack*, White House says, The Washington Post, 9 July 2021.
NPR, *Estonia hosts NATO-led cyber war games, with one eye on Russia*, 2 May 2022.
NATO:
- *Strategic Concept*, 2022a.
- First meeting of NATO national cyber coordinators, 18 May 2022b.
- *Cyber Defence*, 8 July 2021.
- *NATO Cyber Defence*, February 2019.
- *NATO and the EU enhance cyber defence cooperation,* 10 February 2016.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) :
- *Georgia-Russia conflict (2008)*, 17 September 2021a.
- *Microsoft Exchange Server data breach (2021)*, 12 August 2021b.
- *Ukrainian parliamentary election interference (2014)*, 6 July 2021c.
- *Cyber operations against medical facilities*, 15 February 2022.

NATO PA, Committee on Democracy and Security (CDS), *Report :Virtual Visit to Estonia*, 22 April 2021.
NATO PA, *NATO PA President's statement on the attribution of large-scale cyber hacks to China*, 20 July 2021.
Office of the Director of National Intelligence (ODNI), *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, 6 January 2017.
Open-ended working group on developments in the field of information and telecommunications in the context of international security (GTCNL), *Final Substantive Report*, 10 March 2021.
Polityuk, Pavel, *Ukraine suspects group linked to Belarus intelligence over cyberattack*, Reuters, 16 January 2022.
Radio Free Europe (RFE), *Biden Says Russia Has 'Some Responsibility' In Pipeline Ransomware Attack*, 10 May 2021.
Reuters, *Czech election websites hacked, vote unaffected -Statistics Office*, 22 October 2017a.
Reuters, *L'équipe Macron confirme avoir été la cible de cyber-attaques*, 26 April 2017b.
Reynolds, Paul, *'Wizard Spider': Who are they and how do they operate?*, RTE, 19 May 2021.
Rivero, Nicolás, *Hacking collective DarkSide are state-sanctioned pirates*, Quartz, 11 May 2021.
Rundle, James et Stupp, Catherine, *Ukraine Thwarts Cyberattack on Electric Grid, Officials Say,* The Wall Street Journal, 12 April 2022.
Sanchez, Linda, *Bolstering the Resilience of the Alliance Against Disinformation and Propaganda*, NATO PA, 10 November 2021.
Sanger, David and Barnes, Julian, *Biden Signs Executive Order to Bolster Federal Government's Cybersecurity*, The New York Times, 12 May 2021a.
Sanger, David and Barnes, Julian, *United States Indicts Iranian Hackers in Voter Intimidation Effort*, The New York Times, 18 November 2021b.
Sanger, David and Perlroth, Nicole, *U.S. Accuses North Korea of Cyberattacks, a Sign That Deterrence Is Failing*, The New York Times, 26 April 2020.
Sanger, David, Barnes, Julian and Conger, Kate, *As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War*, The New York Times, 28 February 2022.
Sanger, David, *Microsoft Warns of Destructive Cyberattack on Ukrainian Computer Networks*, The New York Times, 16 January 2022.

Schmitt, Michael, *Norm-Skepticism in Cyberspace? Counter-Factual and Counterproductive*, Just Security, 28 February 2020.
Schmitt, Michael, *Russian cyber operations and Ukraine: the legal framework*, Lieber Institute West Point, 16 January 2022.
SHAPE, *Cyber Coalition 2021 Concludes in Estonia*, 6 December 2021.
Siemens, *Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?*, 2021.
Slayton, Rebecca, *What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment*, International Security, 2017.
Smith, David, *The Hillary Clinton email controversy explained: what we know so far*, The Guardian, 1 November 2016.
Srivastava, Mehul, *Inside Ukraine's online defence: the battle against Moscow's cyber attacks*, Financial Times, 24 March 2022.
Srivastava, Mehul, *Russia pummelled by pro-Ukrainian hackers following invasion*, Financial Times, 6 May 2022.
Srivastava, Mehul, Murgia, Madhumita and Murphy, Hannah, *The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion*, Financial Times, 9 March 2022.
The Economist, *Ransomware highlights the challenges and subtleties of cybersecurity*, 19 June 2021.
The Economist, *Russia seems to be co-ordinating cyber-attacks with its military campaign*, 10 May 2022.
The Guardian, *Ukraine says evidence points to Russia being behind cyber-attack*, 16 January 2022.
United Nations Security Council, *Arria-formula Meeting on "Preventing Civilian Impact of Malicious Cyber Activities"*, 19 December 2021.
United Nations General Assembly, *A/C. 1/76/L.13,* 8 October 2021.
Vallance, Chris, *UK blames Russia for satellite internet hack at start of war*, BBC, 10 May 2022.
van der Meer, Sico, *How states could respond to non-state cyber-attackers*, Clingendael, June 2020.
Venkina, Ekaterina, *How Denmark became the most cyber-secure country*, IPS, 2021.
Warrell, Helen, *Czech Republic turns to war-games to build cyber defences*, Financial Times, 18 February 2021.
White House, *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China*, 19 July 2021.