prague
student
summit

BACKGROUND REPORT

Cybersecurity

Magdalena Tetourová
magdalena.tetourova@amo.cz

AMO.CZ

Obsah

1 Preface 3

2 Introduction 3

2.1 Definition of the Cyberspace 3

2.2 Importance of the Cyberspace 4

3 History 5

3.1 Significant attacks 5

3.1.1 Estonia (2007) 5

3.1.2 Georgia (2008) 5

3.1.3 Stuxnet (2010) 5

3.1.4 National Research Council (2014) 6

3.1.5 SolarWinds (2020) 6

3.2 Impact of Cyber Events 6

4 Defence 6

4.1 Passive defence 6

4.2 Active defence 14

4.3 Sovereignty 14

4.4 Law of Armed Conflict (LOAC) 14

4.5 Tallinn Manual 14

4.6 International Law 15

5 Cooperation 15

5.1 Policy & Precautions 15

5.2 NATO Committee 14

5.3 Centre of Excellence 14

6 Future steps 14

6.1 Article 5 14

6.2 Alliance-wide Cyber Operations 14

7 Conclusion 14

8 Questions for negotiations 14

9 Recommended further reading 14

1 Preface

This background report aims to acquaint the reader with the subject of Cyber Defence and Cybersecurity. It is not intended to serve as an all-encompassing or exhaustive exploration of the topic, but rather as a summary of key information. It is strongly advised against concluding your research solely based on this document. The questions and references in the last chapters of this background are there to convey what to focus on while conducting further research. In case of any questions regarding this document, please contact the author at magdalena.tetourova@amo.cz

2 Introduction

In 2016 NATO recognised the cyber domain as one comparable to air, land, sea and space, given the escalating frequency of cyberattacks and their adverse effects on both cyberspace and the physical world. Ensuring cybersecurity is crucial as it safeguards all types of data against theft and loss. This is particularly important while considering sensitive data like protected health information, personally identifiable information, intellectual property, and government or business information systems.[1]

If not safeguarded properly, a leak of these types of data can cause damage, often also of material character. Both NATO and its member states have launched initiatives to better tackle the cyber challenge both operationally and in terms of capability development. Nevertheless, a common approach to cyber defence is still missing among major NATO members.[2]

2.1 Definition of the Cyberspace

Although various different definitions reference cyberspace, this document will focus on two main ones. The first definition views the field primarily from a technical perspective: "Cyberspace refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication. It is a large computer network made up of many worldwide computer networks that employ TCP/IP protocol to aid in communication and data exchange activities. Cyberspace's core feature is an interactive and virtual environment for a broad range of participants."[3]

Contrarily, the second definition views cyberspace simply as "all computer networks of the world", with this non-physical space forming the so-called 5th domain of modern warfare. It considers all types of networks: the internet, other networks, but also even internal systems that are not directly connected to the internet.[4] As such, even the artificial intelligence, autonomous systems and quantum technologies used by the Alliance are considered parts of the cyberspace.[5] [6] [7]

TCP/IP is a pack of protocols used to connect network devices on the internet. It specifies how data are exchanged.[6]

Critical Infrastructure is a collection of systems, networks and public works that a government considers essential to its functioning and the safety of its citizens. The specific infrastructure that each nation considers critical varies. It usually includes electrical grids, public services and communication systems. Special attention must be given to protect critical infrastructure from cyber attacks.[7]

2.2 Importance of the Cyberspace

Cyberwarfare itself doesn't have an official definition, it is a way by which one side of a conflict can do harm to the other side of the conflict via cyberspace.[12] It can for example include the activity of using the internet to attack a country's computers in order to damage things such as communication and transport systems or water and electricity supplies. A crucial distinction is that cyberwarfare is mostly conducted by a military body.[13]

A **cyberattack**, on the other hand, is an intentional violation of cyber security by an individual or an organised group in order to gain information or access to the network of the target.[14]

- A cybercrime is not easily defined, because the law of every state regards it differently. In general, however, cybercrime is conducted by an individual or an organized group in order to enrich itself. Their motives are not political, but purely personal.[15]

- Cyberterrorism can be defined in a very comparable way to a cybercrime. However, there is one difference: Cyberterrorism is politically motivated in order to achieve some kind of a goal.[16]

Cyberwarfare is strongly connected to many aspects of conventional warfare. Nevertheless, in some areas, it completely changes the nature of traditional conflict, or what is considered advantageous in it. For instance, it enables small states to potentially cause bigger damage using cyberwarfare than it would be able to using only its armed forces.[8]

In an era marked by an increasing reliance on interconnected digital systems, the need for cyber defence capabilities has become paramount. Moreover, it is important to understand cyberspace as a constantly evolving domain. It evolves at an incredibly fast pace and even for the most advanced states, it can be complicated to manage.[9] Therefore, cyber defence initiatives hold significant importance in the modern digital era. Cyber threats, including state-sponsored attacks, cyber espionage, and disruptive operations, pose grave risks to national security and critical infrastructure.[10]

The NATO cyber defence policy emphasises the importance of collective defence, resilience, and deterrence in countering cyber threats. Its primary

Cyber defence initiatives hold significant importance in the modern digital era. Cyber threats, including state-sponsored attacks, cyber espionage, and disruptive operations, pose grave risks to national security and critical infrastructure.

objectives include enhancing situational awareness, promoting information sharing and cooperation, developing capabilities, and fostering a cyber defence culture within its member states.[11]

In conclusion, NATO's cyber defence initiatives underline the Alliance's commitment to adapt to the changing security landscape.

3 History

The first chapter of this background laid the foundation of a basic understanding of important cyber concepts. This was achieved through the review of basic concepts relevant to the cyber domain. The understanding of the cyber domain will be further built upon in the upcoming chapter through the examination of significant cyber events through recent history.

3.1 Significant attacks

3.1.1 Estonia (2007)

By 2002, Estonia had issued electronic identification cards to all of its citizens. It was through these cards that Estonians could access government services online, from voting and social security services to filing taxes. By 2007 and 97% of Estonians were using online banking services.[17]

The attacks on Estonia lasted three weeks in April and May 2007 – immediately following the removal of a statue dedicated to Soviet soldiers who died in the Second World War.[18]

Many government websites and civilian services, such as banks and news sites, experienced DDoS attacks. This attack rendered the services unusable by the citizens of Estonia due to the high volume of traffic experienced.[19]

The DDoS reached their peak on 9 May 2007. While the cyber attacks on Estonia have not officially been attributed to Russia, many organisations, including industry and governments, believe Russia was behind the events. US Intelligence and Cyber Law & Business Report have also attributed the actions on Estonia to Russia.[20]

The attacks highlighted an institutional gap and the realisation of the increased threats that exist in the cyber domain. This led to the formal accreditation of the Cooperative Cyber Defense Center of Excellence (CCD COE) by NATO on 14 May 2008. The pinnacle accomplishment of CCD COE to date is the creation of the Tallinn Manual.[21]

3.1.2 Georgia (2008)

The cyber conflict against Georgia in 2008 is an interesting case study where the attacks occurred concurrently with conventional warfare. This was the first time cyber attacks were used in conjunction with kinetic military action.[22] As with events in Estonia, Russia is believed to be involved in this cyber conflict.[23]

The impacts of these cyber attacks were widely felt across the country, impacting many of the services available to the citizens. The attacks successfully denied citizen access to 54 websites related to communications, finance and government.'[24]

The government did not have an effective means to communicate with their citizens as the DDoS attacks impacted not only government websites but also media outlets. This lack of information and communication internally within Georgia, caused either by the cyber attacks or the unintended self-censorship, created panic across the population.[25]

3.1.3 Stuxnet (2010)

In September 2003, the International Atomic Energy Agency (IAEA) board of governors approved a resolution for the suspension of Iran's nuclear program.[26]

However, during the IAEA inspections, it was observed that Iran did not cooperate with the resolutions and it could not be determined whether a nuclear weapons program was underway. The Stuxnet program was then initiated under the George Bush administration, and it became a joint initiative between the US and Israel once Barack Obama took office. The US used the cyber domain as a tool to influence Israel – the possibilities Stuxnet presented persuaded Israel to partner with the Therefore, Israeli intelligence (at the initiative of the US) helped to develop a malware that resulted in material damage to Iran's nuclear facilities.[27]

Stuxnet demonstrated to the world that malware could expand beyond the cyber domain and cause physical damage to infrastructure. Nowadays, it is estimated that the Stuxnet malware was able to infect up to 100 000 computers, 58% of which were located in Iran, but it is believed that other countries were also affected.[28]

3.1.4 National Research Council (2014)

In July 2014, Canada, more specifically the National Research Council (NRC), became the victim of a state-sponsored spear-phishing attack originating from China.[29]

It is unknown exactly what intellectual property China was able to secure; however, the NRC had been working on classified projects at the time, including developing highly secure quantum communications as well as DNA sequencing. In addition to financial and intellectual property implications, the cyber attack also caused political strains.[30]

3.1.5 SolarWinds (2020)

The SolarWinds cyber attack is one of the most recent high-profile cyber prolonged infiltrations, being reported on 17 December 2020 by Microsoft. The attack capitalised on a backdoor that was discovered in the SolarWinds software, a systems management software. Through this backdoor, malicious software was able to be installed, eventually reaching more than 18,000 companies and US government departments.[31]

While the malware was able to reach the US Department of Energy, it was unable to compromise the computer systems. Although not officially attributed, the US government believes Russian intelligence organisations were the main perpetrators of the attack.[32]

3.2 Impact of Cyber Events

In order to understand the topic properly, it is important to note the impact of significant cyber attacks and events.

The attacks on Estonia (2007) resulted in the acknowledgment that more policy and legal frameworks need to be developed in order to effectively and lawfully navigate the cyber domain. The Tallinn Manual was created as one part of the reaction, and is nowadays used by lawmakers and cyber planners as an ethical guide through the cyber domain whenever cyber action is considered.[33]

Stuxnet (2010), considered the first cyber action to cross domain from cyber activities to physical damage, demonstrated the power of intelligence gathering as it relates to cyber planning.[34]

The attack on the Canadian NRC (2014) demonstrated the power of China's ability to gather information and the political strain that may result from it.[35]

Finally, SolarWinds (2020) highlighted the importance of collaboration and intelligence sharing between industrial partners and government organisations.[36]

4 Defence

From a technical point of view, cyber defence is a series of mechanisms and software with one main goal: protect the network that it is integrated in. Cyber defence can be broken down into two categories: passive and active cyber defence.

4.1 Passive defence

Passive cyber defence uses tools such as anti-virus software, firewalls and user education, intending to increase cyber security education and practice of all who use the networks.[37] It can be defined as "measures taken to reduce the probability of, and to minimise the effects of damage caused by hostile action without the intention of taking the initiative".[38]

Passive cyber defence aims to reduce the impact of a cyber attack and decrease the time required to restore the network should the attack be successful.[39]

4.2 Active defence

Active cyber defence encompasses cyber countermeasures and counterattacks directed at a hostile cyber actor. These counter attacks are a defensive response to a cyber attack executed by a hostile actor.

Defensive cyberattacks can be further broken down into two subcategories: mitigative counterstrike and retributive counterstrike.[40]

A mitigative counterstrike would involve actions taken in self-defence in order to interrupt an attack in progress and mitigate immediate harm to a target system. If the goal of the counterstrike is to punish the attacker, it is considered a retributive counterstrike. However, under international law, only the mitigative counterstrike is truly defensive, because its purpose is to defend oneself against an immediate threat.[41]

4.3 Sovereignty

Cyberspace, together with the other four domains (land, sea, air, and outer space) is a reflection of the current international system and, thereby, is largely affected by the rules that characterise it. The issue of state sovereignty in cyberspace raises critical questions about the need to regulate the cyber domain and gradually reach an international cyber order. The cyberspace itself is often characterised as a domain that transcends physical space and thereby is immune to state sovereignty and resistant to international regulation.[42]

This myth is based on a widely-held belief that cyberspace is 'not a physical place' and therefore defies the rules that apply to other domains. Actions in the cyber domain seem to take place 'outside' the state in a 'virtual' manner, but their implications affect the 'real' world, 'inside' states.

However, getting back to the description of cyberspace and the physical layer, it is obvious that cyberspace requires physical infrastructure in order to operate. This infrastructure is terrestrially based and therefore not immune to state sovereignty.[43]

States need to be present in cyberspace and exercise control for reasons of national security. National critical infrastructures like banking and finance, oil and gas, electricity and water, or transportation all depend upon computer networks to operate and therefore cannot escape state control.[44]

4.4 Law of Armed Conflict (LOAC)

An important aspect that should be considered when analysing cyber warfare is the Law of Armed Conflict (LOAC) and its application to the cyber domain. Much of the infrastructure in the cyber domain is considered dual-use, meaning the infrastructure and equipment are used for both civilian and military operations. At some point, it is reasonable to assume that most cyberattacks will transit through, reside or be prepositioned on telecommunications infrastructure used by the civilian population, through communication lines, data centres etc.[45]

The cyberattack's secondary effects are difficult to determine when attacking dual-use systems or equipment. This has an impact on the proportionality factor as it is difficult to anticipate the degree of expected collateral damage. Since the LOAC does not permit an attack if the collateral damage on the civilian population exceeds the military advantage gained given the attack is successful, it is also expected that a commander must anticipate through reasonable means the degree of collateral damage.[46]

Therefore, it could be argued that since the degree of interdependencies between dual-use and civilian infrastructure is so extensive, it is not reasonably feasible to accurately anticipate all the possible secondary effects of a cyberattack. Such attacks could therefore be considered entirely illegal under the LOAC.[47]

4.5 Tallinn Manual

The Tallinn Manual is a non-legally-binding scholarly work by international law academics and practitioners intended to provide an objective restatement of international law as applied in the cyber context. It is policy- and politics-neutral and does not represent the legal position or doctrine of any State or organisation, including the CCD COE.[48] The manual has developed eight criteria to be used when determining if the prohibition of Article 2(4) was broken. However, the manual was not intended to be a definitive guide.[49]

The first version of the Tallinn Manual was centred around cyber war. Tallinn Manual 2.0 was released three years later and expanded to "focus on activities below the level of war, which include cyber terror, cyber espionage, and cybercrime".[50] [51]

The Tallinn Manual attempts to bring the international community together and reach common ground regarding the impact of a cyber attack. It attempts to quell the debate as to if a cyber attack could constitute a use of force and takes a different approach. A cyber attack may not surpass the threshold of use of force, however it could constitute "a violation of the principle of non-intervention in the international affairs of another state". [52]

States need to be present in cyberspace and exercise control for reasons of national security. National critical infrastructures like banking and finance, oil and gas, electricity and water, or transportation all depend upon computer networks to operate and therefore cannot escape state control.

4.6 International Law

A continuing issue writ large within both NATO and the global community involves how existing international law applies to activities in cyberspace. From a security perspective, significant progress was made with the publication of the Tallinn Manual on the International Law Applicable to Cyber Warfare (2013).[53]

Perhaps not surprisingly, some non-NATO states, Russia and China in particular, do not fully agree with the principles espoused within the Tallinn Manual. This is a significant challenge, especially considering these countries are two of the five permanent members of the United Nations Security Council.[54]

However, NATO initiatives with the private sector also present significant legal issues, especially in regards to the status of the private contractors' civilian employees who support NATO operations. The implications of their vulnerability to legitimate attack as well as liability for due diligence remain under legal evaluation.[55]

5 Cooperation

5.1 Policy & Precautions

The main tasks of NATO are collective defence, crisis management and cooperative security amongst its member states. The new Enhanced Cyber Defence Policy affirms the role that NATO cyber defence contributes to the mission of collective defence and embraces the notion that a cyberattack may lead to the invocation of Article 5 actions for the Alliance. However, the truth is that most cyberwarfare activity is right below the threshold of what would be probably perceived as an armed conflict.[56]

But when does a cyberattack cross the line of the threshold of armed conflict? Rule 30 of the Tallinn Manual defines a cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[57] The legal test on whether a cyber-incident has crossed the line of an armed conflict is 'effects-based,' focusing on the nature and extent of the injury and damage caused on a case-by-case basis and whether it has caused death or destruction. An attack would generally not be considered to have crossed the line when it is reversible or temporary.[58]

The largest part of **NATO Cyber Defence Policy** is made of Alliance members' Cyber Defence Pledge, which was signed as part of the 2016 Warsaw Summit. Members of the Alliance pledged to further enhance cyber defence capabilities and to improve the process

of education, training and awareness in the area of cyber defence.[59]

There is a big desire to have a rather sovereign cyber infrastructure on national level that is also capable of defensive and offensive activities in a coordinated manner. The Cyber Defence Pledge is a crucial aspect of the further development of NATO's cyber capabilities.[60]

5.2 NATO Committee

The Cyber Defence Committee has been operating since 2014 (it was established by renaming the Defense Policy and Planning Committee). This committee operates under the authority of the North Atlantic Council and its main goal is to administer NATO's cyber defence policy.[61]

It cooperates with the Cyber Defense Management Board (CDMB), which is an organ responsible for strategic planning, executive direction regarding the topic of NATO networks and its cyber security.[62] The CDMB is composed of political leaders and important military, operational and technical personnel and institutions that are mainly responsible for the cyber defence of NATO. It is connecting civilian and military bodies to achieve the highest possible effectiveness.[63]

5.3 Centre of Excellence

Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia is a multi-nationally sponsored entity, which offers recognized expertise and experience to the benefit of the Alliance. Centres of Excellence (COEs) are international military organisations that train and educate leaders and specialists from NATO member and partner countries. The idea to establish such a multinational centre originated in 2004 and moved forward also due to the cyberattack against Estonia in 2007.[64]

The CCD COE is composed of multiple bodies, with the main body being the Steering Committee. It is then divided into the following branches: Technology, Strategy, Operations, Law, Education & Training, and Support. The mission of the CCD COE is to enhance the cooperative cyber defence capability of NATO and its nations, thus improving the Alliance's interoperability in the field of cooperative cyber defence.[65]

- Participation open to all NATO nations; access open to Partners;
- Tangible improvement to NATO capabilities;
- No duplication/competition with NATO command arrangements;
- No NATO command and control (the head of the committee is an Estonian chairman).[66]

6 Future steps

6.1 Article 5

Concerning the cyber domain, NATO ultimately reaffirms its nature of defensive alliance, as well as the principle for which international law is also applicable to cyberspace.[67]

It is worth noting how NATO declares itself ready to use not only cyber capabilities, but also air, maritime or land capabilities to counter a cyberattack. For the purpose of deterrence and defence, NATO thus considers all operational domains in an integrated manner, in line with the integration of the Cyber Operation Centre into the NATO command structure.

In order to perform effective deterrence, however, the ability to assign the authorship of attacks is fundamental – a priority which demands further efforts on behalf of the Allies.[68] In conventional warfare, distinguishing an act of war and what is not is pretty much straightforward. However, in cyberspace, there are no solid boundaries of what is perceived as an act of war. For example, in Estonia, Russia targeted governmental websites and did significant damage. Was it an act of war?

Even though it is often possible to track the perpetrator of an attack via an IP address, it is complicated and in many cases almost impossible to reliably determine the attacker. The most important lesson to draw is that NATO might need to adapt its primary task of collective defence to cyber defence.[69]

6.2 Alliance-wide Cyber Operations

The 2019 London Summit gave a new politico-strategic impulse to NATO's activities in cyberspace, in light of the geopolitical competition with China and Russia. Secretary General Jens Stoltenberg declared that the "cyberspace is the new battleground and making NATO cyber ready is a top priority". Indeed, Stoltenberg highlighted that cyber threats will become more dangerous with the development of new technologies, such as AI and machine learning. These technologies are fundamentally changing the nature of warfare – to an extent comparable to the industrial revolution.[70]

Accordingly, the 2020 report of the NATO 2030 Reflection Group ascribed great relevance to Emerging and Disruptive Technologies (EDTs), understood both as a sector in which to invest more, and a set of challenges. Within EDTs, those related to cyber defence, above all Artificial Intelligence (AI), are considered a priority.[71]

The new Strategic Concept, defined throughout 2021, pays great attention to cyber defence, cyber domain and EDTs as another field of confrontation with China and Russia.[72] As one NATO cyber officer noted, "NATO has established a capable defence for most cyber threats, but that is just the first step, what needs to quickly follow is the development of 'active defence' capabilities".[73]

In conventional warfare, distinguishing an act of war and what is not is pretty much straightforward. However, in cyberspace, there are no solid boundaries of what is perceived as an act of war.

The Alliance must be able to dissuade and deter threats to its members, from whatever source and across all domains, while being prepared to defend all parts of NATO territory and to protect the critical functions of Allied societies. Such operations extend far beyond the military dimension, incorporating political, economic, technological, social, and psychological considerations.[74]

7 Conclusion

Through the examination of significant cyber events in history, some important conclusions can be drawn:

- Collateral damage and intended consequences are a serious consideration when operating in the cyber domain;
- A legal and ethical framework is critical for operating the cyber domain;
- The safeguard of information is crucial to preserving intellectual property and national interests.

Finally, the examples of specific cyber events demonstrated the importance of collaboration, not only between government departments but also with industry partners and allies. Collaboration improves both the probability of uncovering a cyberattack and the swift resolution of its aftermath.

An important aspect to be considered when analysing cyber warfare is also the Law of Armed Conflict (LOAC). It could be argued that since the degree of interdependencies in the cyber domain is so extensive, it is not possible to accurately anticipate all the secondary effects of a cyberattack. Such attacks could therefore be considered illegal under LOAC.[75]

The debate becomes more complex when considering the theory that an attack on national critical infrastructure could be actually considered a threat, by extension, a use of force. Consistent with its current Cyber Defence Policy, NATO's top priority

is to protect its own communications and information systems that support alliance military operations.[76]

However, a significant issue for NATO´s cyberspace operations is the possibility of offensive actions carried out by the Alliance.[77] The Tallinn Manual now provides one framework to evaluate cyber actions, ensure they are ethical and legal, and its use is not limited for the purpose of the Alliance.

Cyberspace activities are currently one of NATO's top priorities. While there will always be room for improvement and the priorities of member states regarding this matter often differ, the continued resourcing for, and pursuit of improved cyberspace capabilities will help to ensure the steady progress of NATO cyberspace endeavours.[78]

8 Questions for negotiations

I. What are a member state's cyber warfare capabilities?
II. Is a member state willing to offer its capabilities?
III. How does a member state perceive sovereignty in cyberspace?
IV. What is a member state's stance on the topic of Article 5 in relation to cyberspace?
V. How should NATO proceed in case of an invocation of Article 5 due to a cyberattack?
VI. How should NATO respond in case of a cyberattack by a private individual or a terrorist group in comparison to an attack by another country?
VII. Where is the difference between a cyber act of war and just a 'provocation'?
VIII. Should civilian or military personnel be responsible for cyberspace?
IX. What ground rules for offensive cyber warfare should NATO have?

9 Recommended further reading

Cyber Defence. Online. North Atlantic Treaty Organization. 2023. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm. [cit. 2024-02-26].

The Tallinn Manual. Online. CCD COE. 2023. Available at: https://ccdcoe.org/research/tallinn-manual/. [cit. 2024-02-26].

Emerging and disruptive technologies. Online. North Atlantic Treaty Organization. 2023. Available at:: https://www.nato.int/cps/en/natohq/topics_184303.htm. [cit. 2024-02-19].

Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare. Online. CCD COE. 2013. Available at: https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE. [cit. 2024-02-26].

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Online. Cambridge University Press. 2017. Available at: https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9. [cit. 2024-02-26].

KLIMBURG, Alexander. National Cyber Security Framework Manual. Online. CCD COE. 2012. Available at: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf. [cit. 2024-02-19].

Pražský studentský summit

Pražský studentský summit je unikátní vzdělávací projekt existující od roku 1995. Každoročně vzdělává přes 300 studentů středních i vysokých škol o současných globálních tématech, a to především prostřednictvím simulace jednáníčtyř klíčových mezinárodních organizací – OSN, NATO, EU a G20.

Asociace pro mezinárodní otázky

AMO je nevládní nezisková organizace založená v roce 1997 za účelem výzkumu a vzdělávání v oblasti mezinárodních vztahů. Tento přední český zahraničně politický think-tank není spjat s žádnou politickou stranou ani ideologií. Svou činností podporuje aktivní přístup k zahraniční politice, poskytuje nestrannou analýzu mezinárodního dění a otevírá prostor k fundované diskusi.

Magdalena Tetourová

Autorka je spolupracovnicí Asociace pro mezinárodní otázky a členkou přípravného týmu Pražského studentského summitu.

Autor: Magdalena Tetourová
Imprimatur: Pavel Tichý, Anna Marie Podlipná
Jazyková úprava: Barbora Trčková, Aleš Khol
Faktická korektura: Matěj Hulička
Sazba: Dominik Merta
Grafická úprava: Jaroslav Kopřiva
Vydala Asociace pro mezinárodní otázky (AMO) pro potřeby XXIX. ročníku Pražského studentského summitu.

Asociace pro mezinárodní otázky (AMO)
Žitná 27, 110 00 Praha 1
Tel.: +420 224 813 460
e-mail: summit@amo.cz
IČ: 65 99 95 33
www.amo.cz
www.studentsummit.cz

References

[1] KELLEY, Karin. What is Cybersecurity and Why It is Important? Online. Simplilearn. 2023. Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security. [cit. 2024-02-19].

[2] MARRONE, Alessandro and SABATINO, Ester. Cyber Defence in NATO Countries: Comparing Models. Online. Istituto Affari Internazionali. 2021. Available at: https://www.iai.it/en/pubblicazioni/cyber-defence-nato-countries-comparing-models. [cit. 2024-02-19].

[3] ROUSE, Margaret. Cyberspace. Online. Techopedia. 2023. Available at: https://www.techopedia.com/definition/2493/cyberspace. [cit. 2024-02-19].

[4] SCHREIER, Fred. On Cyberwarfare. Online. Geneva Centre for Security Sector Governance (DCAF). 2015. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf. [cit. 2024-02-19].

[5] Emerging and disruptive technologies. Online. North Atlantic Treaty Organization (NATO). 2023. Available at: https://www.nato.int/cps/en/natohq/topics_184303.htm. [cit. 2024-02-19].

[6] SHACKLETT, Mary. What is TCP/IP? Online. TechTarget. 2021. Available at: https://www.techtarget.com/searchnetworking/definition/TCP-IP. [cit. 2024-02-19].

[7] WRIGHT, Gavin. Critical Infrastructure. Online. TechTarget. 2023. Available at: https://www.techtarget.com/whatis/definition/critical-infrastructure. [cit. 2024-02-19].

[8] Cyberwarfare. Online. Journal of Information Warfare. 2020. Vol. 19, No. 4, 12 p. Available at:https://www.jstor.org/stable/27033642. [cit. 2024-02-19].

[9] Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace. Online. Texas National Security Review. 2020. Available at: http://dx.doi.org/10.26153/tsw/10224. [cit. 2024-03-04].

[10] SHEA, Jamie. Cyberspace as a Domain of Operations. Online. MCU Journal. 2018, Vol. 9, No. 2, 18 p. Available at: https://apps.dtic.mil/sti/pdfs/AD1068701.pdf. [cit. 2024-02-19].

[11] ATKINSON, Ryan. NATO Cyber Defence, 2000-2022. Online, Thesis and Dissertation Repository. The University of Western Ontario, 2023. Available at: https://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=12219&context=etd. [cit. 2024-02-19].

[12] Cyber Warfare. Online. Cambridge Dictionary. 2020. Available at: https://dictionary.cambridge.org/dictionary/english/cyber-warfare. [cit. 2024-02-19].

[13] BUXTON, Oliver. Cyber Warfare: Types, Examples, and How to Stay Safe. Online. Avast. 2023. Available at: https://www.avast.com/c-cyber-warfare. [cit. 2024-02-19].

[14] What Is a Cyberattack? Online. Cisco. 2023. Available at: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html. [cit. 2024-02-19].

[15] KLIMBURG, Alexander. National Cyber Security Framework Manual. Online. CCD COE. 2012. Available at: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf. [cit. 2024-02-19].

[16] What Are the Most Common Cyber Attacks? Online. Cisco. 2023. Available at: https://ciscolivewem.cisco.com/c/en_in/products/security/common-cyberattacks.html. [cit. 2024-02-19].

[17] Allied Command Operations. Online. North Atlantic Treaty Organization (NATO). 2023. Available at: https://www.nato.int/cps/en/natohq/topics_52091.htm. [cit. 2024-02-19].

[18] LUCAS, George. Ethics and Cyber Warfare. 1. Oxford University Press, 2017. ISBN 9780190276522.

[19] LIAROPOULOS, Andrew. War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory. Online. ProQuest. 2010. Available at: https://www.proquest.com/docview/869506998?%20Proceedings&sourcetype=Conference%20Papers%20. [cit. 2024-02-19].

[20] SHAKARIAN, Paulo; SHAKARIAN, Jana and REUF, Andrew. Introduction to Cyber-Warfare: A Multidisciplinary Approach. Syngress, 2013. ISBN 978-0-12-407814-7.

[21] The Tallinn Manual. Online. CCD COE. 2023. Available at: https://ccdcoe.org/research/tallinn-manual/. [cit. 2024-02-26].

[22] Group of experts presents report to Secretary General. Online. North Atlantic Treaty Organization (NATO). 2020. Available at: https://www.nato.int/cps/en/natohq/news_179730.htm. [cit. 2024-02-19].

[23] Russian Cyber Strategy and the War Against Georgia. Online. Atlantic Council. 2014. Available at: https://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia/. [cit. 2024-02-19].

[24] IASIELLO, Emilio. Russia' s Improved Information Operations: From Georgia to Crimea. Online. US Army War College (USAWC). 2017. Available at: https://press.armywarcollege.edu/parameters/vol47/iss2/7/. [cit. 2024-02-19].

[25] DEIBERT, Ronald. Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. Online. Security Dialogue. 2012, Vol. 43, No. 1, 22 pages. Available at: https://www.jstor.org/stable/26301960. [cit. 2024-02-19].

[26] MASTERSON, Julia. IAEA Report Demonstrates Urgent Need to Restore JCPOA. Online. Arms Control Association. 2022. Available at: https://www.armscontrol.org/author/julia-masterson. [cit. 2024-02-19].

[27] LINDSAY, John. Stuxnet and the Limits of Cyber Warfare. Online. Taylor and Francis. 2013. Available at: https://www.tandfonline.com/doi/abs/10.1080/09636412.2013.816122. [cit. 2024-02-19].

[28] CHEN, Thomas. Lessons from Stuxnet. Online. Research Gate. 2011. Available at: https://www.researchgate.net/publication/260534719_Lessons_from_Stuxnet. [cit. 2024-02-19].

[29] BRONSKILL, Jim. Chinese hackers attacked National Research Council computers. Online. CTV News. 2014. Available at: https://www.ctvnews.ca/canada/chinese-hackers-attacked-national-research-council-computers-1.2146400?cache=. [cit. 2024-02-19].

[30] BOUTILIER, Alex. Canadian spy agency says China hacked into National Research Council computers. Online. Toronto Star. 2014. Available at: https://www.thestar.com/news/canada/canadian-spy-agency-says-china-hacked-into-national-research-council-computers/article_79b1fc42-be7b-5a50-87c4-0adcac8b5e8b.html. [cit. 2024-02-19].

[31] OLADIMEJI, Saheed. SolarWinds hack explained: Everything you need to know. Online. TechTarget. 2023. Available at: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know. [cit. 2024-02-19].

[32] WALTON, Robert. DOE confirms its systems were compromised by SolarWinds hack. Online. Industry Dive. 2020. Available at: https://www.utilitydive.com/news/doe-confirms-its-systems-were-compromised-by-solarwinds-hack/592441/. [cit. 2024-02-19].

[33] The Tallinn Manual. Online. CCD COE. 2023. Available at: https://ccdcoe.org/research/tallinn-manual/. [cit. 2024-02-26].

[34] CHEN, Thomas. Cyberterrorism After Stuxnet. Online. US Army War College. 2014. Available at: https://www.jstor.org/stable/resrep11324. [cit. 2024-03-04].

[35] Minister of Foreign Affairs appearance before the House of Commons Special Committee on Canada-China Relations (CACN) – Briefing material. Online. Government of Canada. 2023. Available at: https://www.international.gc.ca/transparency-transparence/briefing-documents-information/parliamentary-committee-comite-parlementaire/2020-11-23-canada-china-chine.aspx?lang=eng. [cit. 2024-03-04].

[36] LEPAGE, Melany. Ethics in a Dangerous Cyberspace Time. Online. Canadian Forces College. 2021. Available at: https://www.cfc.forces.gc.ca/259/290/23/286/Lepage.pdf. [cit. 2024-02-19].

[37] ROUSE, Margaret. Cyber Defense. Online. Techopedia. 2024. Available at: https://www.techopedia.com/definition/6705/cyber-defense. [cit. 2024-02-26].

[38] CHEN, Zhuo. Law of War and Its Applicability in the Area of Cyber World. Online. Research Gate. 2022. Available at: https://www.researchgate.net/publication/360495055_Law_of_War_and_Its_Applicability_in_the_Area_of_Cyber_World. [cit. 2024-02-26].

[39] Joint Publication 1-02. Online. Department of Defense. 2016. Available at: https://irp.fas.org/doddir/dod/jp1_02.pdf. [cit. 2024-02-26].

[40] MEJIA, Eric. Act and Actor Attribution in Cyberspace Online. United States Air Force. 2014. Available at: https://www.jstor.org/stable/26270607. [cit. 2024-02-26].

[41] KESAN, Jay and Carol HAYES. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace]. Online. University of Illinois. 2011. Available at: https://www.researchgate.net/publication/228256871_Mitigative_Counterstriking_Self-Defense_and_Deterrence_in_Cyberspace. Research Paper. [cit. 2024-02-26].

[42] LIAROPOULOS, Andrew. Exercising State Sovereignty in Cyberspace. Online. Journal of Information Warfare. 2013. Vol. 12, No. 2, 8 pages. Available at: https://www.jstor.org/stable/26486852. [cit. 2024-02-26].

[43] HEINTSCHEL VON HEINEGG, Wolff. Legal Implications of Territorial Sovereignty in Cyberspace. Online. Europa-Universität, Frankfurt. CCD COE. 2012. Available at: https://www.ccdcoe.org/uploads/2012/01/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf. [cit. 2024-02-26].

[44] FRANZESE, Patrick. Sovereignty In Cyberspace: Can It Exist? Online. Trade Journal. 2009. Vol. 64, No. 1, 42 pages. Available at: https://www.proquest.com/docview/195182873?sourcetype=Trade%20Journals. [cit. 2024-02-26].

[45] MEJIA, Eric. Act and Actor Attribution in Cyberspace. Online. United States Air Force. 2014. Available at: https://www.jstor.org/stable/26270607. [cit. 2024-02-26].

[46] LIAROPOULOS, Andrew. War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory. Online. ProQuest. 2010. Available at: https://www.researchgate.net/publication/287453228_War_and_ethics_in_cyberspace_Cyber-conflict_and_just_war_theory. [cit. 2024-02-26].

[47] MEJIA, Eric. Act and Actor Attribution in Cyberspace. Online. United States Air Force. 2014. Available at: https://www.jstor.org/stable/26270607. [cit. 2024-02-26].

[48] The Tallinn Manual. Online. CCD COE. 2023. Available at: https://ccdcoe.org/research/tallinn-manual/. [cit. 2024-02-26].

[49] LUCAS, George. Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare. Online. Oxford University Press. 2016. Available at: https://doi.org/10.1093/acprof:oso/9780190276522.001.0001. [cit. 2024-03-04].

[50] NATO Centres of Excellence. North Atlantic Treaty Organization. 2023. Available at: https://www.nato.int/cps/en/natohq/topics_68372.htm. [cit. 2024-02-26].

[51] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Online. Cambridge University Press. 2017. Available at: https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9. [cit. 2024-02-26].

[52] FISCHER, Kristian and Hans MOURITZEN. Danish Foreign Policy Review 2022 has been published. Online. Danish Institute for International Studies. 2022. Available at: https://www.diis.dk/en/research/danish-foreign-policy-review-2022-has-been-published. [cit. 2024-02-26].

[53] FOCARELLI, Carlo. Self-defence in cyberspace. Online. Edward Elgar Publishing. 2015. Available at: https://ideas.repec.org/h/elg/eechap/15436_12.html. [cit. 2024-02-27].

[54] Current Members. Online. United Nations Security Council. 2014. Available at: https://www.un.org/securitycouncil/content/current-members. [cit. 2024-02-27].

[55] GREEN, James. Cyber Warfare - A Multidisciplinary Analysis. Routledge. 2016. ISBN 9780415787079.

[56] Joint Publication 1-02. Online. Department of Defense. 2016. Available at: https://irp.fas.org/doddir/dod/jp1_02.pdf. [cit. 2024-02-26].

[57] Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare. Online. Cambridge University Press. 2013. Available at: https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE. [cit. 2024-02-26].

[58] HODGKINSON, Sandra. Crossing the Line. Online. The International Lawyer. 2018. Vol. 51, No. 3, 16 pages. Available at: https://www.jstor.org/stable/27009647. [cit. 2024-02-26].

[59] Cyber Defence. Online. North Atlantic Treaty Organization. 2023. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm. [cit. 2024-02-26].

[60] Cyber Defence Pledge. Online. North Atlantic Treaty Organization. 2016. Available at: https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en. [cit. 2024-02-26].

[61] Cyber Defence. Online. North Atlantic Treaty Organization. 2023. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm. [cit. 2024-02-26].

[62] CATON, Jeffrey. NATO Cyberspace Capability: A Strategic and Operational Evolution. Online. US Army War College. 2016. Available at: https://press.armywarcollege.edu/monographs/423/. [cit. 2024-02-26].

[63] About Us. Online. CCD COE. 2023. Available at: https://ccdcoe.org/about-us/. [cit. 2024-02-26].

[64] Cyber Defence. Online. North Atlantic Treaty Organization. 2023. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm. [cit. 2024-02-26].

[65] Allied Command Operations (ACO). Online. North Atlantic Treaty Organization. 2023. Available at: https://www.nato.int/cps/en/natohq/topics_52091.htm. [cit. 2024-02-26].

[66] Centres of Excellence. Online. North Atlantic Treaty Organization. 2024. https://www.nato.int/cps/en/natohq/topics_68372.htm. [cit. 2024-02-26].

[67] KOCH, Robert. How Anonymous Is the Tor Network? A Long-Term Black-Box Investigation. Online. Universität der Bundeswehr. 2016. Available at: https://www.researchgate.net/publication/298331354_How_Anonymous_Is_the_Tor_Network_A_Long-Term_Black-Box_Investigation. [cit. 2024-02-27].

[68]Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Online. Cambridge University Press. 2017. Available at: https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9. [cit. 2024-02-26].

[69] Statement by the North Atlantic Council concerning malicious cyber activities. Online. North Atlantic Treaty Organization. 2020. Available at: Statement by the North Atlantic Council concerning malicious cyber activities, 03-Jun.-2020 - Nato.int https://www.nato.int/cps/en/natohq/official_texts_176136.htm. [cit. 2024-02-27].

[70] FISCHER, Kristian and Hans MOURITZEN. Danish Foreign Policy Review 2022 has been published. Online. Danish Institute for International Studies. 2022. Available at: https://www.diis.dk/en/research/danish-foreign-policy-review-2022-has-been-published. [cit. 2024-02-26].

[71] NATO will defend itself. Online. North Atlantic Treaty Organization. 2019. Available at: https://www.nato.int/cps/en/natohq/news_168435.htm. [cit. 2024-02-27].

[72] Group of experts presents report to Secretary General. Online. North Atlantic Treaty Organization. 2020. Available at: https://www.nato.int/cps/en/natohq/news_179730.htm. [cit. 2024-02-27].

[73] The EU Security Union Strategy. Online. European Commission. 2024. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en. [cit. 2024-02-27].

[74] CATON, Jeffrey. NATO Cyberspace Capability: A Strategic and Operational Evolution. Online. US Army War College. 2016. Available at: https://press.armywarcollege.edu/monographs/423/. [cit. 2024-02-26].

[75] MEJIA, Eric. Act and Actor Attribution in Cyberspace. Online. United States Air Force. 2014. Available at: https://www.jstor.org/stable/26270607. [cit. 2024-02-26].

[76] Bucharest Summit Declaration. Online. North Atlantic Treaty Organization. 2008. Available at: https://www.nato.int/cps/en/natolive/official_texts_8443.htm. [cit. 2024-02-27].

[77] Item 1416 - Briefing – Tackling New Security Challenges. Online. North Atlantic Treaty Organization. 2011. Available at: https://archives.nato.int/briefing-tackling-new-security-challenges-2. [cit. 2024-02-27].

[78] Key Priorities. Online. North Atlantic Treaty Organization. 2020. Available at: https://www.nato.int/cps/en/natohq/85291.htm. [cit. 2024-02-27].