

# NATO Cyber Defense

Ladislav Švábek  
ladislav.svabek@amo.cz



AMO.CZ



# 1 PREFACE

This background report is supposed to introduce you, the reader to the topic of Cyber Defense. It is not to be considered an exhaustive or comprehensive work on this topic but rather a summary of the most essential information. You are highly recommended to not stop your research by reading this document (more on that in the last chapter of this background), especially for the purposes of writing a high-quality position paper. Seeing that this might seem like an overwhelming task at first, the questions included in the penultimate chapter of this background are designed to help the reader to better grasp the fundamentals and also to show what to concentrate on. In case of any questions or remarks concerning this document, please contact the author at *ladislav.svabek@amo.cz*

## 2 INTRODUCTION

### 2.1 Definition of cyberspace

First of all, we need to define what cyberspace is. There are numerous definitions that refer to cyberspace, but for the purpose of this work, two of them will be mentioned.

Definition A considers cyberspace from a technical point of view and can come in handy in certain situations:

“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.”<sup>28</sup>

In the case of definition B, we can define cyberspace as non-physical space, or so-called 5th domain of modern warfare. All of the networks, computers and even internal systems that are not connected to the Internet, at least not directly, are part of cyberspace. In this definition we can see a glimpse of what cyberspace means in the modern world, regarding the international security.<sup>1</sup>

TCP/IP is a pack of protocols (standard set of rules that allows devices to communicate with each other<sup>26</sup>) used to connect network devices on the internet. It specifies how data are exchanged.<sup>27</sup>

### 2.2 Importance of cyber defense

Cyber threats and attacks are nowadays becoming a more common way how to damage your competitors or weaken their infrastructure. In the light of recent events, cyberattacks have been a part of hybrid warfare. Because cyberattacks do not respect state borders, all members of the Alliance must be equally prepared to repel any future cyberattack. The Alliance is built on a few principles, one

of which is the Article 5, concerning collective defense, and cyber defense plays a crucial part in it. Cyberwarfare has been acknowledged as the 5th domain of war, in which article 5 can be invoked.<sup>2</sup> Also, with technology developing further and further, NATO needs to keep up with the rapidly changing environment of cyberspace.

**Hybrid warfare** “blends conventional/unconventional, regular/irregular, and information and cyber warfare.” Hybrid warfare combines multiple dimensions of war in order to destabilise a state and polarize its society to achieve what the attackers want.<sup>29</sup>

### 2.3 Key concepts

Cyberattack (or cyber attack) is an intentional violation of cybersecurity by an individual or an organised group in order to gain information or access to the network of the target.<sup>3</sup> Depending on the context of the attack, we recognize cyber warfare, cyber terrorism and cybercrime.

**Cyberwarfare** itself does not have any exact official definition. Nevertheless, here is how it can be generally conceived: Cyberwarfare is a way by which one side of a conflict can do harm to the other side of the conflict via cyberspace. What is crucial is that cyberwarfare is mostly conducted by a military body.

**Cybercrime** is also not easily defined, because every state has different laws regarding that. In general, however, cybercrime is conducted by an individual or an organised group in order to enrich itself. Their motives are not political, but purely personal.<sup>4</sup>

**Cyberterrorism** can be defined in a very similar way as cybercrime. However, there is one difference. Cyberterrorism is politically motivated in order to achieve some kind of a goal.<sup>5</sup>

#### Chosen methods of cyberattacks and used software

(There are dozens of ways how an attacker can conduct an attack. For the purpose of this document, only a few were chosen.)

**Distributed denial of service (DDoS)** is an attack using a botnet (network of computers or devices that have been infected, including even smart devices, for example a smart fridge) in order to overwhelm the targeted network with loads of requests that result in malfunction of the said system or website.

**Malware** is any software whose main principle is malicious behaviour. For instance, the attacker can gain access to personal files and information.<sup>33</sup>

**Website defacement** means that the attacker changes the content of websites without the permission of the owner. These can have a strong political motivation.<sup>34</sup>

**Keylogger** has two variants, either physical or virtual. The main principle is to monitor user's keystrokes to determine his login information, thus gain access to his private accounts.<sup>31</sup>

**Data/security breach** is a complete breach of a systems' security. Attacker usually finds a vulnerability and uses it to steal data or information. With this method, previous types of attacks are usually combined together and used in order to achieve higher effectivity.<sup>32</sup>

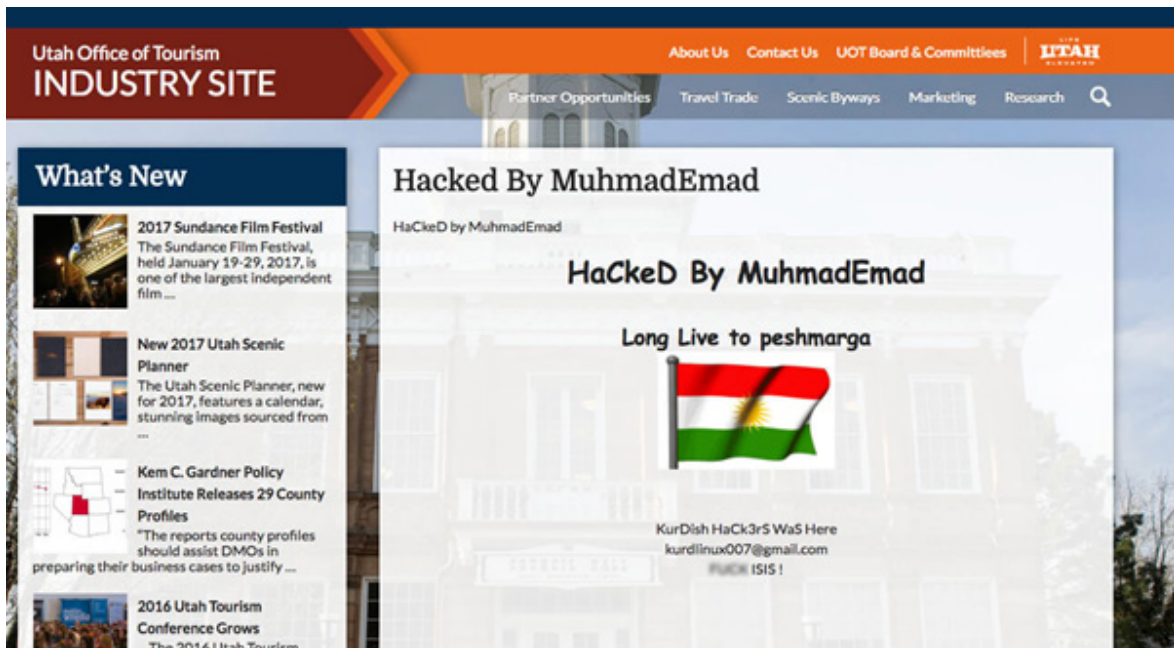


Figure 1. website defacement example<sup>30</sup>

### 3 CYBER WARFARE HISTORY

Should we examine the beginnings of cyber warfare, we would have to start in the Cold War era. To be more specific, in 1982 when the CIA successfully conducted a cyberattack against the Soviet Union. This attack was not a direct attack against the Soviet pipeline system, actually it was conducted in a rather special way. CIA let a Soviet spy steal a compromised program, which they have later on installed in Siberia. As a result, the Soviet pipeline in Siberia exploded.<sup>6</sup>

This attack is classified as a logical bomb (malicious program that is dormant until certain preset requirements are met). Going more into the present, first actual cyberwarfare happened during the wars in Chechnya (1994; 1997-2001), when both parties used cyberspace, mainly the Internet, to convince the public that their side is the right one.

However, this cyberwarfare was rather an example of an information war than hacking of government networks,

although Russia did indeed hack Chechen websites.<sup>7</sup> Following Chechnya, there was cyberwarfare in Kosovo (1999), that was also mainly in the form of an information war. However, Serbian hackers still managed to hack NATO's computers and the website of the White House.<sup>8</sup>

From these examples, we can deduce that cyberwarfare is closely tied to information wars and that nations are using both of these tactics in order to achieve the best results possible. Of course, there were many more conflicts which included cyberwarfare, but for the purposes of this work, only a few of them are mentioned. With that being said, where there was an armed conflict, there was cyberwarfare.

### 3.1 Significant attacks in general

One of the attacks that is worth mentioning is an attack on Iranian nuclear facilities. Malware called Stuxnet, created probably by U.S.-Israeli joint efforts because it seemed suspiciously suited for a certain type of software, infiltrated numerous industrial plants that were closely tied to the fabrication of nuclear weapons. This virus has been effectively sabotaging the process of enriching uranium for a few weeks.<sup>9</sup>

We can only guess for how long the Iranian nuclear weapons research was delayed. However, that virus later got out of these facilities and spread over the Internet, although it did not do any harm to other networks and computers.<sup>10</sup> The paradox is that this cyberattack was initially conducted physically by an employee that had to connect a USB stick to the facility network. Stuxnet is nowadays recognized as one of first large scale offensive cyber weapons.<sup>11</sup>

Another significant event in cyberwarfare happened more recently, in May 2019. An organised group of hackers that

claimed to be a part of Hamas tried to conduct a cyber offensive against Israel. As a response, Israel tracked and located the exact location of this hacker group and performed and airstrike on a building that the attack allegedly came from.<sup>12</sup> This action was unique, because it was the first physical retaliation after getting cyberattacked by a foreign power.

### 3.2 2007 attack on Estonia

Probably the most famous attack ever was on Estonia in May 2007. This attack had its origins in Russia and the reason for it might seem rather harmless. The Estonian government decided to move a monument of the sacrifice of Soviet Armed forces from World War II. to a different place. This act was not very well accepted by the Russian Minority in Estonia, which turned to protests later on.

During the protests and after them, DDoS attacks were conducted firstly against government websites, which ultimately led to the shutdown of the Estonian Ministry of Foreign Affairs and Ministry of Justice websites. A few days later, attackers targeted private networks like banks and other financial institutions, which also led to a shutdown of these and significant losses from a financial point of view.

These attacks are an example of what cyberwarfare is capable of, not just because they endured for a few weeks, but also because Russia was never held responsible for it. It is necessary to point out that these DDoS attacks were not only conducted by Kremlin agents but also by ordinary Russian people, since a "call to arms" spread throughout Russian social media. Consequently, it led to a creation of the NATO Cooperative Cyber Defense Center of Excellence

**Information war(fare)** has many definitions, that can be perceived in a military, technical or civilian way. It is composed of numerous activities, typically a support of fake news and intentional internet trolling in order to support one's agenda. In general, the ultimate goal of information warfare is to make one's competitor unable to find consensus on the most important topics or to influence the population of one's competitor, so that the state loses its stability. The biggest perpetrator of these tactics in Europe currently is Russia. In combination with cyberwarfare, information warfare can be a lethal tactic that can disrupt the functioning of a state even before a single soldier steps onto its territory.<sup>35</sup>

(CCD COE) in May 2008, but more about that later.<sup>13</sup>

## 4 CYBER DEFENSE

From a technical point of view, cyber defense is a series of mechanisms and software with one main goal, to protect

a network that it is integrated in. Cyber defense needs to be adaptable and ready to respond to possible threats imme-

diately. Tracking the attacker is also a part of cyber defense mechanisms.<sup>14</sup>

## 4.1 NATO Policy on Cyber Defense

In 2011, NATO Defense Ministers approved the NATO Policy on Cyber Defense. That policy's main focus is the protection of NATO's communication and information systems. Thus, NATO is actively enhancing its capabilities to deal with a broad spectrum of cyber threats it currently faces.<sup>15</sup>

In 2016 NATO reaffirmed its defensive mandate and recognized cyberspace as a key part of its operations. This means that NATO will treat with cyberattacks, if they are "big enough", the same way it would treat land, sea or air attacks on a NATO member. In case of a cyber "warfare" which would include Alliance members, article 5 would be invoked. This is a crucial aspect of cyber defense structure of NATO, since all Alliance members must treat cyber warfare as a credible threat.

It is important to note what is meant by "big enough". In conventional warfare, what is 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. Is it an act of war? What is more, even though it is possible to track the perpetrator of an attack via an IP address, it is complicated and in some cases maybe impossible to reliably determine the attacker. If Russia would bomb governmental buildings, it would surely be an act of war, but in cyberspace, it is very hard to define the borderline. So while talking about cyberattack being big enough, in the same way as other domains of war, it would need to cause significant damage to the infrastructure of NATO or its member states. Last but not least, most of cyberwarfare activity is right below the threshold of what would probably be perceived as an armed conflict.<sup>16</sup>

Biggest part of NATO Cyber Defense policy is made of Alliance members' Cyber Defense Pledge. This pledge was signed by member states' representatives in July 2016, at the NATO Summit in Warsaw. Members of the Alliance pledged to further enhance cyber defense capabilities and to improve the process of education, training and awareness in the area of cyber defense. To be more specific, education plays a very important part of NATO's cyber defense strategy both on the international level as well as on the level of each individual member state. The Pledge aims to improve cyber defense of member states on all levels and it contains crucial information on the topic of cyber defense that you are highly recommended to read thoroughly.<sup>17</sup>

Last but not least, at the Brussels Summit in July 2018, the topic of cyber defense has also been discussed. The Alliance leaders re-acknowledged that cyber defense is a crucial part of collective defense. NATO furthermore works

on the implementation of cyberspace as a domain of operations (such as land, air, sea and space). It was stated that "individual Allies may consider, when appropriate, attributing malicious cyber activity and responding in a coordinated manner, recognising attribution is a sovereign national prerogative." This means that 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. Furthermore, the Alliance pointed out that the Cyber Defense Pledge is a crucial aspect of the further development of NATO's cyber capabilities.<sup>18</sup>

## 4.2 Precautions against cyberattacks

NATO's main interest in cyber defense is the protection of its own networks. For that reason, NATO is applying procedures to effectively protect itself. For example, there is a NATO Computer Incident Response Capability (NCIRC), based in Mons, Belgium. This body is supposed to provide constant support on the topic of cyber defense. We can expect further development of this body alongside the rapidly changing trends in cyberspace.<sup>19</sup>

One of the next precautions are Smart Defense Initiatives. Smart Defense connects all NATO member states together. The main goal is to ensure that states which could not afford to do research in cyberspace, will be able to keep pace with more wealthy and resourceful competitors. This initiative includes Malware Information Sharing Platform (MISP), the Smart Defense Cyber Defense Capability Development (MN CD2) project, and the Multinational Cyber Defense Education and Training (MN CD E & T) project.<sup>20</sup>

Furthermore, in order to be prepared, NATO Cyber Rapid Reaction teams are on standby to assist any member of the Alliance if necessary, 24 hours a day, if requested and approved.<sup>21</sup>

## 4.3 Cyber Defense Committee

The Cyber Defense Committee is a body that is subordinate to the North Atlantic Council. It is working since 2014, when it was agreed to rename the Defense Policy and Planning Committee to Cyber Defense Committee. Its main goal is to administer NATO's cyber defense policy. It cooperates with Cyber Defense Management Board (CDMB), which is a board that has responsibility for strategic planning, executive direction regarding the topic of NATO networks and its cyber security.<sup>22</sup> CDMB is composed of leaders of the policy and important military, operational and technical personnel and institutions that are mainly responsible for cyber defense of NATO. It is connecting civilian and military bodies to achieve the highest possible effectivity.<sup>23</sup>

## 5 COOPERATIVE CYBER DEFENSE CENTRE OF EXCELLENCE (CCD COE)



Figure 2. Scheme of the CCD COE branches<sup>37</sup>

Cooperative Cyber Defense Centre of Excellence (CCD COE) is a cyber defense hub. It is fully accredited and is supported by NATO member states. Its establishment dates back to May 2008 and it is based in Tallinn, Estonia. The idea to establish such a centre originated in 2004 and with the aforementioned attack against Estonia in 2007, the project was realised as its relevance suddenly seemed all the greater. From 2008 to this day, the main goal of CCD COE is to improve capabilities of cooperation and sharing of information inside NATO. CCD COE is composed of multiple bodies, with the main body being

“Centres of Excellence (COEs) are international military organisations that train and educate leaders and specialists from NATO member and partner countries.”<sup>36</sup>

the Steering Committee.

The Steering Committee organises CCD COE’s activities. Moreover, it controls the budget and has the main word on the centre’s policy and all operations that are conducted by CCD COE. It is composed of one representative, with the right to vote, for each Sponsoring Nation. The head of the committee is a chairman from Estonia.<sup>24</sup>

CCD COE is divided into these branches: Technology, Strategy, Operations, Law, Education & Training, and Support.

## 6 FUTURE STEPS OF NATO’S CYBER DEFENSE

It is hard to figure out the future steps of NATO regarding the issue of cyber defense, since a big part of the information is classified. In spite of that, we still know some basic steps for NATO cyber defense in the future. At the Brussels Summit in 2018, it was decided to establish a new Cyberspace Operations Centre (COC).<sup>25</sup> This centre will

serve as a hub for the coordination of NATO’s cyber defense activities and, if necessary, can be used to conduct offensive actions in the field of cyberspace.

One of the main goals of NATO will be to find a consensus regarding cyber warfare principles in relation to Article 5. Because the question of how severe a cyberattack must

be to become eligible for the invocation of Article 5 is still up in the air, it should be the Alliance's main goal to resolve as soon as possible. As mentioned previously, it is hard to distinguish what exactly is an armed conflict in cyber space and what is just a provocation. In case of a cyberattack, there is also an important aspect of who was behind it: Was it a "lone wolf", a group or an enemy state? And should it be

a state, will NATO be able to respond to it? And in what way should it respond?

Last but not least, the Alliance needs to solve how it will guarantee cyber security for all of its member states and furthermore, how to connect and use the individual states' cyberwarfare capabilities for Alliance-wide operations and how to coordinate them.

## 7 CONCLUSION

As already mentioned, cyberwarfare is strongly connected to other aspects of conventional warfare. However, it is necessary to point out that cyberwarfare is mitigating the advantages of a conventional war. For example, a small state can cause bigger damage using cyberwarfare than it would be able to with just its armed forces. With a very small chance of being exposed, it makes cyberwarfare an even more popular way of settling disputes.

In order for NATO to work effectively, it is crucial for member states to fulfill pledges that they have made throughout the years. Because only in that way will they be able to work as an Alliance. Moreover, it is important to understand cyberspace as a constantly evolving domain. In comparison with other do-

mains (sea, land, air and space), it evolves at an incredibly fast pace and even for the most advanced states, it can be complicated to manage.

NATO stands in front of numerous problems in the field of cyberspace, both legislative and strategic and it needs to find a consensus. Otherwise, it will not be as effective as it could be. Last but not least, connecting the cyber capabilities of all the member states willing to contribute may be very tricky, but it is also an important aspect of NATO's cyber defense capabilities.

We strongly recommend the reader to not stop his or her research with this work, but to further study this very broad and interdisciplinary topic. The first step for writing a position paper are the questions and sources below.

## 8 FUNDAMENTAL QUESTIONS

1. What are your country's cyber warfare capabilities?
2. What is your country's stance on the topic of Article 5 in relation to cyberspace?
3. How should NATO proceed in case of a invocation of article 5 due to a cyberattack?
4. What is your country doing to secure its cyberspace?
5. Is your country willing to offer its cyber warfare capabilities?
6. Where is the difference between a cyber act of war and just an "unpleasant provocation"?
7. Should every country have its own "Centre of Excellence"?
8. 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?
9. Should civilian or military personnel be responsible for cyberspace?
10. What ground rules for offensive cyber warfare should NATO have?
11. Should NATO as an organization share cyber technologies among its members, and among partners outside the Alliance?



## 9 RECOMMENDED SOURCES

**Basic factsheet about NATO's cyber defense:**

[https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/pdf\\_2019\\_02/20190208\\_1902-factsheet-cyber-defence-en.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf)

**More in-depth information about cyber defense, history and NATO's policy. Highly recommended to read:**

[https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm)

**A video summarizing the history and present of cyber warfare threats:**

<https://www.youtube.com/watch?v=lbpCLOXPiC4>

**A documentary focused on U.S.-Israeli malware called Stuxnet:**

<https://www.imdb.com/title/tt5446858/>

**NATO library list that includes cybersecurity strategy articles about every member nation:**

<https://ccdcoe.org/library/strategy-and-governance/>

**Nato Review article on the role of cyberspace:**

<https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm>

## RESOURCES

- 1 SCHREIER, Fred. On Cyberwarfare [online]. Nato multimedia library: Nato multimedia library, 2015 [cit. 2019-09-10]. Available at: <https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf> pages 10-11
- 2 NATO's role in cyberspace: Cyber in focus. NATO Review [online]. 2019 [cit. 2019-09-11]. Available at: <https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm>
- 3 What Are the Most Common Cyber Attacks?. Cisco [online]. Online: Cisco, 2019 [cit. 2019-09-11]. Available at: <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>
- 4 KLIMBURG, Alexander, ed. National Cyber Security framework manual. Online: 2012. ISBN 978-9949-9211-2-6. Available at: [https://ccdcoe.org/uploads/2018/10/NCSFM\\_o.pdf](https://ccdcoe.org/uploads/2018/10/NCSFM_o.pdf) pages 13-15
- 5 What Are the Most Common Cyber Attacks?. Diplomacy [online]. Online: Diplomacy.edu, 2019 [cit. 2019-09-11]. available at: <https://www.diplomacy.edu/blog/cyberterrorism-what-are-we-not-talking-about>
- 6 Reagan Approved Plan to Sabotage Soviets. Washington Post [online]. 2004 [cit. 2019-09-11]. Available at: <https://www.washingtonpost.com/archive/politics/2004/02/27/reagan-approved-plan-to-sabotage-soviets/a9184eff-47fd-402e-beb2-63970851e130/>
- 7 SCHREIER, Fred. On Cyberwarfare [online]. Nato multimedia library: Nato multimedia library, 2015 [cit. 2019-09-10]. Available at: <https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf> pages 107-108
- 8 GEERS, Kenneth. Cyberspace and the Changing Nature of Warfare. CCD COE [online]. 2018 [cit. 2019-09-11]. Available at: [https://ccdcoe.org/uploads/2018/10/Geers2008\\_CyberspaceAndTheChangingNatureOfWarfare.pdf](https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf) page 6
- 9 Timeline: How Stuxnet attacked a nuclear plant. BBC [online]. 2019 [cit. 2019-09-11]. Available at: <https://www.bbc.com/timelines/zc6fbk7#z32pycw>
- 10 Stuxnet was work of U.S. and Israeli experts, officials say. Washington Post [online]. 2012 [cit. 2019-09-11]. Available at: [https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U\\_story.html](https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html)
- 11 Stuxnet Facts Report: A technical and Strategic Analysis. CCD COE [online]. Tallinn, 2012 [cit. 2019-09-11]. Available at: [https://ccdcoe.org/uploads/2018/10/Falco2012\\_StuxnetFactsReport.pdf](https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf) pages 26-28
- 12 What Israel's Strike on Hamas Hackers Means For Cyberwar. Wired [online]. 2019 [cit. 2019-09-11]. Available at: <https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/>
- 13 SCHREIER, Fred. On Cyberwarfare [online]. Nato multimedia library: Nato multimedia library, 2015 [cit. 2019-09-10]. Available at: <https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf> pages 109-110
- 14 Cyber Defense. Technopedia [online]. 2019 [cit. 2019-09-11]. Available at: <https://www.techopedia.com/definition/6705/cyber-defense>
- 15 Cyber Defense. North Atlantic Treaty Organisation [online]. NATO, 2018 [cit. 2019-09-10]. Available at: [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm)

- 16 NATO's role in cyberspace. NATO Review magazine [online]. NATO, 2019, 12/02/2019 [cit. 2019-09-25]. Available at: <https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm>
- 17 Cyber Defence pledge. North Atlantic Treaty Organization [online]. 2016 [cit. 2019-09-10]. Available at: [https://www.nato.int/cps/en/natohq/official\\_texts\\_133177.htm](https://www.nato.int/cps/en/natohq/official_texts_133177.htm)
- 18 Brussels Summit Declaration. North Atlantic Treaty Organization [online]. NATO, 2018 [cit. 2019-09-10]. Available at: [https://www.nato.int/cps/en/natohq/official\\_texts\\_156624.htm#20](https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20)
- 19 Cyber Defense. North Atlantic Treaty Organisation [online]. NATO, 2018 [cit. 2019-09-10]. Available at: [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm)
- 20 Smart Defence. North Atlantic Treaty Organisation [online]. NATO, 2017 [cit. 2019-09-10]. Available at: [https://www.nato.int/cps/ua/natohq/topics\\_84268.htm#](https://www.nato.int/cps/ua/natohq/topics_84268.htm#)
- 21 Cyber Defense. North Atlantic Treaty Organisation [online]. NATO, 2018 [cit. 2019-09-10]. Available at: [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm)
- 22 North Atlantic Treaty Organisation. The NATO Cooperative Cyber Defence Centre of Excellence [online]. CCD-COE, 2019 [cit. 2019-09-10]. Available at: <https://ccdcoe.org/organisations/nato/>
- 23 Cyber Defense. North Atlantic Treaty Organisation [online]. NATO, 2018 [cit. 2019-09-10]. Available at: [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm)
- 24 About us. CCDCOE [online]. CCDCOE, 2019 [cit. 2019-09-10]. Available at: <https://ccdcoe.org/about-us/>
- 25 NATO cyber command to be fully operational in 2023. Reuters [online]. 2019 [cit. 2019-09-11]. Available at: <https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9>
- 26 Protocol. Techterms [online]. Sharpened Productions, 2019 [cit. 2019-09-06]. Available at: <https://techterms.com/definition/protocol>
- 27 TCP/IP (Transmission Control Protocol/Internet Protocol). Techtarget [online]. TechTarget, 2019 [cit. 2019-09-06]. Available at: <https://searchnetworking.techtarget.com/definition/TCP-IP>
- 28 Cyberspace. Technopedia [online]. Techopedia, 2019 [cit. 2019-09-06]. Available at: <https://www.techopedia.com/definition/2493/cyberspace>
- 29 Hybrid war - does it even exist?. NATO [online]. NATO, 2016, 2016 [cit. 2019-09-25]. Available at: <https://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/>
- 30 Website defacement image. Wordfence [online]. [cit. 2019-09-13]. Available at: [https://www.wordfence.com/wp-content/uploads/2017/02/utahOfficeOfTourism\\_defaced.jpg](https://www.wordfence.com/wp-content/uploads/2017/02/utahOfficeOfTourism_defaced.jpg)
- 31 Keylogger. Technopedia [online]. 2019 [cit. 2019-09-11]. Available at: <https://www.techopedia.com/definition/4000/keylogger>
- 32 What is a security breach?. Norton [online]. 2019 [cit. 2019-09-11]. available at: <https://us.norton.com/internetsecurity-privacy-security-breach.html>
- 33 Common types of cyber attacks. Cisco [online]. Online: Cisco, 2019 [cit. 2019-09-11]. Available at: <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>

34 Defacement. Technopedia [online]. 2019 [cit. 2019-09-11]. Available at: <https://www.techopedia.com/definition/4870/defacement>







35 GILES, Keir. Handbook of Russian Information Warfare [online]. Rome, Italy: DeBooks Italia srl., 2016 [cit. 2019-09-11]. ISBN 978-88-96898-16-1. Available at: <http://www.ndc.nato.int/download/downloads.php?icode=506> pages 6-11

36 Centres of Excellence. North Atlantic Treaty Organisation [online]. NATO, 2019 [cit. 2019-09-10]. Available at: [https://www.nato.int/cps/en/natolive/topics\\_68372.htm](https://www.nato.int/cps/en/natolive/topics_68372.htm)

37 Schematic of CCD COE image. CCD COE [online]. [cit. 2019-09-13]. Available at: <https://ccdcoe.org/uploads/2018/11/struktur-web-2-1.svg>

## 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 jednání tří klíčových mezinárodních organizací – OSN, NATO a EU.

-  [studentsummit.cz](http://studentsummit.cz)
-  [summit@amo.cz](mailto:summit@amo.cz)
-  [facebook.com/studentsummit](https://facebook.com/studentsummit)
-  [instagram.com/praguestudentsummit](https://instagram.com/praguestudentsummit)
-  [twitter.com/studentsummit](https://twitter.com/studentsummit)
-  [youtube.com/studentsummit](https://youtube.com/studentsummit)

## Asociace pro mezinárodní otázky (AMO)

AMO je nevládní nezisková organizace založená v roce 1997 za účelem výzkumu avzdělávání 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.

## Ladislav Švábek

Autor je spolupracovníkem Asociace pro mezinárodní otázky a členem přípravného týmu Pražského studentského summitu.

<p>POŘADATEL</p>  <p><b>AMO.CZ</b></p>	<p>GENERÁLNÍ PARTNER</p>  <p>The Kellner Family Foundation</p>
<p>TOP PARTNEŘI</p>     <p>Zastoupení v České republice</p>  	
<p>PARTNEŘI</p>    <p>Embassy of Canada Ambassade du Canada</p>     <p>UNITED NATIONS Informační centrum OSN v Praze</p>     	
<p>MEDIÁLNÍ PARTNEŘI</p>  	

**Autor:** Ladislav Švábek

**Imprimatur:** František Novotný, Tomáš Kosub, Tomáš Rezek, Ondřej Kovanda

**Jazyková úprava:** Klára Kloučková

**Sazba:** Andrea Tunysová

**Grafická úprava:** Jaroslav Kopřiva

**Vydala Asociace pro mezinárodní otázky (AMO) pro potřeby XXV. ročníku Pražského studentského summitu.**

© AMO 2019

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](http://www.amo.cz)

[www.studentsummit.cz](http://www.studentsummit.cz)