Received: 3. 10. 2022 Accepted: 14. 10. 2022 Published on-line: 16. 12. 2022
Available from: www.obranaastrategie.cz doi: 10.3849/1802-7199.22.2022.02.036-050

M.A.D. Znovu? Posun termínu M.A.D. do kybernetické domény

M.A.D. Again? Shift of the Term M.A.D. to the Cyber Domain

Aleš Tesař[a], *Fabian Baxa*[b], *Dalibor Procházka*[c]

Abstrakt

Článek přináší nový význam akronymu M.A.D. (Mutually Assured Destruction – vzájemně zaručené zničení) v oblasti bezpečnosti. Z původní spojitosti s jadernou problematikou se jeho využití přesouvá do sféry kybernetického prostoru. Text seznamuje se základním dělením domén důležitých pro lidské aktivity. Vysvětluje jejich význam z hlediska nepopiratelné využitelnosti a dostupnosti pro lidskou společnost, současně upozorňuje na zranitelnost a nutnost zajištění jejich ochrany. Podrobněji se věnuje nové páté doméně – kyberprostoru. V této souvislosti jsou zmiňovány bezpečnostní hrozby a naznačovány některé právní aspekty vyplývající z této dimenze.

Abstract

The article introduces a new meaning of the acronym M.A.D. (Mutually Assured Destruction) in the field of security. From the original connection with nuclear issues, its use is moving to the area of cyberspace. The text introduces the basic division of domains important for human activities. It explains their importance in terms of undeniable usability and availability for mankind, at the same time, it draws attention to their vulnerability and the need to ensure their protection. It deals in more details with the new fifth domain – cyberspace. In this context, security threats are mentioned and some legal aspects are indicated.

Klíčová slova

Kybernetický útok; kyberprostor; kyberzločin; kybernetická válka; doména; celosvětové veřejné statky; vzájemně zaručené zničení.

Keywords

Cyberattack; cyberspace; cybercrime; cyberwar; domain; global commons; mutually assured destruction.

[a] Centre for Security and Military Strategic Studies, University of Defence. Brno, Czech Republic. E-mail: ales.tesar@unob.cz. 0000-0002-8175-430.
[b] Centre for Security and Military Strategic Studies, University of Defence. Brno, Czech Republic. E-mail: fabian.baxa@unob.cz. 0000-0003-4030-0406.
[c] Centre for Security and Military Strategic Studies, University of Defence. Brno, Czech Republic. E-mail: dalibor.prochazka@unob.cz. 0000-0002-6601-0012.

INTRODUCTION

In the 1980s, the president of the United States Ronald Reagan and Soviet general secretary Mikhail Gorbachev agreed that both countries were owners of nuclear arsenals able to guarantee the Mutually Assured Destruction of both countries and the whole world. This negotiation has not only contributed the acronym M.A.D. to the international policy discourse but also an acknowledgment of the fact that it is not necessary to have capabilities to destroy everything several times when one time is enough. This idea was expressed by one of the former Soviet leaders, Nikita Khrushchev, in talks with the president of the United States, John Fitzgerald Kennedy. This realization led to a series of treaties limiting nuclear arsenals on both sides to agreed numbers, such as the INF[1] and START I[2] treaties. Another detail concerning these treaties is the fact that no other nuclear country is a signatory of these treaties.

In the present time, a new understanding of M.A.D. can be interpreted. It is not linked to nuclear weaponry of the two engaged sides nor other nuclear powers, but it can be seen in connection with the impossibility to use effectively global commons in general, at least one of the domains of human activities, in practice. The expression "destruction" in the cyber domain does not necessarily have to mean a permanent, physical annihilation of all means and networks used in this domain but also blocking or substantial worsening of the exploitation of this domain for a certain period. The main domains in which human activities are carried out are generally considered to include land, sea, air, space, and cyberspace, however some others will be indicated in the article. Some of the newly considered domains, esp. cyberspace, are not defined yet world-wide, like the first three domains, land, sea, and air.

The global common domains, in general, should be usable by all mankind, thus, equal access to them should be ensured for all. Therefore, everyone should have the right to access and use all of them. To ensure this right, it is necessary to have these domains under the control of humanity, in the sense that no individual could abuse it. Controlling of these domains, important for the realization of human activities, often critical to the existence of mankind, represents a significant influence on world security. Restrictions on that right of access can therefore be regarded as a serious security threat.

Within the scope of human activities, it is necessary to bear in mind that they also include military activities. Although threats affect all domains, there is one of them, where the vulnerability is more significant these days. Currently, the meaning of the acronym MAD has shifted from nuclear issues to activities in the cyber field. The aim of this article is to point out the growing importance of the cyber domain for activities of a human civilisation and the possibility of causing critical economic damages due to its vulnerability. This article underlines the necessity to have an appropriate treaty containing the principles and rules of exploitation of this domain applicable world-wide for all users.

[1] INF – Intermediate-Range Nuclear Forces. *Federation of American Scientists* [on-line]. n.d. [cit. 2022-05-19]. Available at: https://nuke.fas.org/control/inf/index.html
[2] START I – Strategic Arms Reduction Treaty. *Federation of American Scientists* [on-line]. n.d. [cit. 2022-05-19]. Available at: https://nuke.fas.org/control/start1/index.html

The effort to reach the aim of this article required usage of several methods, starting from the research of available literature and sources in general, linked with their content analysis, together with deduction and synthesis, and eventually induction to formulate appropriate findings.

GLOBAL COMMONS DOMAINS

Global commons

This expression is taken from medieval English expression "commons" marking everything in a village that was common to all its inhabitants, e.g., roads, crossroads, squares, if any, etc. It originated from the ancient Roman property law *res communis omnia*. In a broader thinking, these assets in the village might be used also by foreigners travelling through the village. In the further text, the term "global commons" is understood as a sum of specific areas, domains (land, sea, air, etc.) where human civilisation carries out its activities, regardless whether these domains are controlled by legislation recognised by the human society in general.

What is the meaning of using commonly owned (owned by the global population), but not only by population, owned and used by everything living on this planet? One can say only human beings can be owners of something, but in human history, this approach has changed several times. Indigenous people on newly discovered islands and even in the continent named America were people who were not recognised as human beings and therefore they were not counted as the owners of the territory they lived on. At that time, one chief of an Indian tribe being asked to sell the territory occupied by his people created the famous idea that land has no owner and therefore is not possible to sell.[3] This deep idea might be understood in the sense that all living creatures around the globe, including people, are only users of the world and its individual domains and the use of them might lead to the right and freedom to use them by an appropriate way.

Land

This domain contains all continents, all ground on this planet, that the human civilisation as well as all living organisms use for their activities. It may be limited by owners' rights and regulated by individual states. Without the land domain, it is not possible to use effectively any other domains. This form of exploitation can be manifested, for example, by airfields, sea ports, space centres, etc.

Sea

The sea domain, sometimes also called the *maritime domain*, is the second area that human civilisation historically set out to explore. Therefore, the use of this domain was an object of series of international treaties. These treaties set the rules of the common use of oceans and seas, such as the territorial (brown) waters or international (blue)

[3] Native Americans Describe Traditional Views of Land Ownership. In: *SHEC: Resources for Teachers*. [on-line] n.d. [cit. 2022–11–02]. Available at: https://tinyurl.com/yw62u687

waters, known as the high seas. These rules were disputed many times but the general concept is accepted, such as the *Geneva Convention on the High Seas*,[4] etc.

Air

The air has been another "commons" for the population worldwide and there are known attempts at formulating the rules how to use this domain to be profitable for everybody. The *Paris Convention*[5] from 1919 and *Chicago Convention*[6] from 1944 should be mentioned here. The use of the air domain is conditioned not only by the use of the land domain, but also by maritime platforms, such as aircraft carriers.

Space

This domain, recognised as a continuation of the air space starting approximately at the height of 100 kilometres[7] from the Earth's surface, is further divided into inner space and outer space. Exploration of the space domain is possible solely through the air domain from the land or sea domains.

In connection with the world security, there are treaties banning the use of this domain for deployment of offensive military systems as well as nuclear weapons. However, they do not forbid the use of conventional military systems for defensive purposes. This legal framework was adopted during the Cold War era. One of the most important legal regulations is the *Outer Space Treaty*[8] from 1967. Up to what level these treaties are respected today is hard to express. Ever arguing purely militarily, the recognisance based on satellite platforms in general is an important combat support activity needed for both defensive as well as offensive actions. Satellite-based communication and navigation can be characterised the same way.

Cyberspace

The newest candidate aspiring to be a member of the global commons family is called cyberspace. This domain is closely linked to the internet as a phenomenon and result as well as a tool of the information age. The cyberspace is considered to be an environment for transporting and processing information in digital form worldwide for all its users. According to the Czech *Act on Cyber Security*,[9] cyberspace means "*a digital environment*

[4] *Geneva Convention on the High Seas*. Geneva [on-line]. 1958. [cit. 2022-05-19]. Available at: https://tinyurl.com/msukhb9d

[5] *Convention Relating to the Regulation of Aerial Navigation*: Paris Convention. Paris [on-line]. 1919. [cit. 2022-07-02]. Available at: https://bit.ly/3Fy3GD6

6 *Convention on International Civil Aviation*. Chicago [on-line]. 1944. [cit. 2022-07-11]. Available at: https://bit.ly/3uXKo54

[7] So called the Kármán Line. *Astronomy Magazine* [on-line]. 2021. [cit. 2022-09-19]. Available at: https://bit.ly/3hxBqs8

[8] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*. London, Moscow, Washington [on-line]. 1967. [cit. 2022-08-11]. Available at: https://bit.ly/3Fz7yUf

[9] The Act No 181/2014 Coll. on Cyber Security and change of related acts (Act on Cyber Security). In: *Collection of Laws*, 2014.

enabling the creation, processing and exchange of information, consisting of information systems, and electronic communications services and networks."[10]

The transportation of information exploits wire as well as wireless means and platforms placed in all physical domains. Using wireless transportation of information, the cyberspace is supported by the electromagnetic spectrum. Conventions and treaties regulating the use of the cyberspace are more and more needed, however, the necessary discussion, negotiation, formulation, and agreement process including all state, non-state as well as private actors - users of this domain - is expected to be lengthy and complicated.

The e*lectromagnetic domain* may be considered to be a part of the environment used by the cyber domain. What counts here as the "commons" is an environment of electromagnetic (EM) waves radiation, sometimes called "ether". This domain is vitally important for all users of any electric device exploring wireless communication starting from radios, TV, GSM mobile phones, GPS, Wi-Fi, Bluetooth, etc. There are conventions dealing with the purpose of use of various bands and frequencies. Lack of respecting them leads to mutual interferences and problems for users of the EM spectrum. This domain still needs the recognition similar to the others.

The "Internet of Things" and "Industry 4.0" mean radical growth of number of devices using the internet in semiautomatic or fully automatic mode, various sensors informing the respective supervising element about their situation, state of wear, failure, etc. The revolution, which is referred to in the use of the term "Industry 4.0", will certainly appear in the military field, too, where it is expected to be called, e.g., "Army 4.0". This revolution makes it possible to plan maintenance and spare parts much more efficiently, which will make operating costs more efficient.

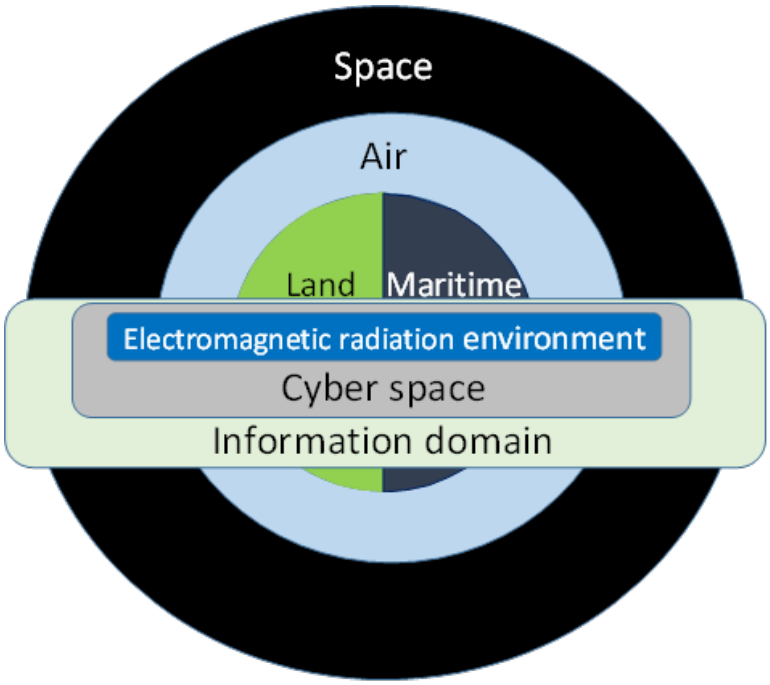
The wireless transmission is mostly used here, what significantly increases the vulnerability of these systems and increases the efficiency of cyberattacks. The *Tallinn Manual* defines the cyberattack as "*a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to object".*[11] These systems generally have the same vulnerabilities as all other systems that use wireless networks. The vulnerability of these networks and the possibility of their use against the opponent was indicated by Bogdanov in his work.[12]

Information

Some countries, e.g., the United States[13] have recognised the information domain as a specific area. This domain is not physically existent compared to the previous other domains. Its main task is to ensure the collection, processing, and distribution of information to users (information cycle).

[10] Ibid. §2 letter a).
[11] *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. 2013. ISBN 978-1-107-02443-4. p. 106. Available also at: https://bit.ly/3BDbSk8
[12] BOGDANOV, S.A. *Monografiya radioelektronnaya borba v voynah I vooruzhennyh konfliktah* [online]. 2007 [cit. 2022-09-02]. Available at: https://tinyurl.com/yhkcb5jd
[13] *Joint Concept for Operating in the Information Environment (JCOIE)*. United States Department of Defense [on-line] 2018. [cit. 2022–07–19]. Available at: https://tinyurl.com/5bwdx3x2

Figure 1: Illustration of various domains of human activities within the Global Commons concept



Source: Authors, modified with the use of *AFDP 3-12 Air Force Doctrine Publication. Cyberspace Operations*. Curtis E. Lemay Center [on-line]. 2011, p. 19. [cit. 2022-07-19]. Available at: https://tinyurl.com/mr3pkjhc

All of the mentioned domains may be also considered domains for military activities due to the fact that the military is part of human activities. The basic task of the military is to secure its own activities and to deny the activities of its opposers in general.

CYBERSPACE AND SECURITY IMPACTS

Present human civilisation vitally needs all of the above mentioned domains for its existence and with the growing level of modernisation, together with globalisation, it is even impossible to see everyday life without the possibility of using these "global commons", including the still inevitable parts of the human civilisation as disputes, conflicts, armed conflicts, and wars. Military experts recognised very quickly that the limitation of access to individual domains will decrease the capabilities of the adversary from the economic, politic, military as well as social point of view and defined the concept of A2/AD (Anti Access/Area Denial). This approach can be applied in all domains

in general, including the cyber domain.[14] This concept has been originally focused on a specific area of (military) operations but today, being focused on the cyber domain, too, the area of operation in cyberspace might include the whole globe. Consequences might be catastrophic for the global economy, critically affecting also the social, medical, and therefore also political dimensions of many developed post-industrial countries. In other words, all countries in the Euro-Atlantic region.

The space as well as cyber domains, in contrary to land, sea, and air ones, are characterised by their specific features. Considering the post Westphalian model of the state,[15] an armed attack against a state territory could be launched through state borders at sea, at land, or entering into the state's airspace using or misusing the neighbouring country territory. The space or cyberspace offer the possibility of attacking a country via running cyber operations or by a single cyber offensive action, without being a direct neighbour of the attacked country. Certainly, when a state deploys sensors as a part of its Information Communication Systems (ICS), including those deployed on the orbit/inner space, with a capability to control or at least to monitor the cyberspace traffic, such a state can become aware in time. On the other hand, smaller states without a proper space programme need to rely on others or they might be attacked by surprise. Recently, several private companies have demonstrated the same capability regarding the deployment of sensors on the orbit, certainly without the same level of responsibility for their misuse as the states.

There might happen a similar situation like in the 1980s, where the main global superpowers might recognise that to keep a suitable economic, social as well as political conditions within their sphere of influence and considering they are able to block major economic development via denying access to the vital domains of human activities, they may also agree, for the sake of acceptable life conditions, that within the developed part of the world it is necessary to mutually assure access to all domains of human activities. Otherwise, massive social unrest within their own population or region-wide conflicts might cause political trembling threatening their present positions and interests.

There was no consensus on the introduction of cyberspace as the fifth domain. As cyber operations gradually became an integral part of conflict resolution, they also started to appear in military doctrines. Among the first to recognize cyberspace as a separate war domain was the U.S. Department of Defence in 2006.[16]

Critics of the recognition of cyberspace as a specific area argued that cyberspace cannot be defined separately, but that it intervenes or interweaves with all other war domains and is inextricably linked to them. Supporters of the new trend, on the other hand, emphasized the need for more effective organization of the armed forces for operations

[14] RUSSELL, Alison Lawlor. Strategic Anti-Access/Area Denial in Cyberspace. In: *2015 7th International Conference on Cyber Conflict* [on-line]. 2015. [cit. 2022-11-03]. Available at: https://tinyurl.com/4w3r859w

[15] MINES, Keith, W. Force Size for the Post-Westphalian World. In: *Orbis* [on-line] 2005. [cit. 2022-10-31]. Available at: https://www.sciencedirect.com/science/article/pii/S0030438705000670

[16] National Military Strategy for Cyberspace Operations. In: *Homeland Security Digital Library* [on-line] 2006. [cit. 2022-11-02]. Available at: https://www.hsdl.org/c/abstract/?docid=35693

in cyberspace, and saw one of the ways in the implementation of cyberspace into military doctrines.[17]

Aside from the controversy over whether cyberspace deserves a separate area of warfare, the fact is that NATO recognized cyberspace as "the domain for operations"[18] at the Warsaw Summit in 2016.[19] Now, from the point of view of the North Atlantic Treaty Organization, cyberspace stands as a separate domain, next to the land, sea, air, and space domains.

The declaration of cyberspace as a separate domain was subsequently reflected in the organizational structures of the armed forces and the associated creation of capabilities. Within the Army of the Czech Republic, the forces were expanded to include cyber forces and, in terms of command and control, the Cyber Forces Command was established. At the same time, the capabilities of the Army of the Czech Republic with the required state of 2030 were determined, which means for the cyber forces to ensure cyber security and defence, including planning, managing, and conducting cyber operations in cyberspace at the tactical level and, in cooperation with military intelligence, conducting cyber operations at the operational level.[20]

Specificities of particular subjects

Related to security, it is necessary to mention that *underdeveloped countries* are not so dependent on space or cyberspace, while they still may have capabilities to launch limited attack via cyberspace. Hence, these countries are not so keen to limit their possibilities by signing any treaty that would provide stability within the existing world as they are not able to explore these domains at the same level as the *economically developed states*.

Already today, there are *private persons, non-state actors (including proxies, criminal organizations, state sponsored actors*) and *commercial organisations* having these capabilities as well as intending to attack state organisations for various reasons. States have to consider this threat. Certainly, states may have more possibilities of recruiting suitable personnel and acquiring the required hardware and software and to coordinate cyber activities with other measures to increase their effectiveness. On the other hand, some non-state as well as commercial organisations have higher level security or defence capabilities than small countries, therefore, the same situation can be expected also in the cyberattack field.

Another difference between state and non-state actors is in the legality of *offensive actions* against other states or organisations. Although not all states comply with all treaties and even their internal rules, almost all states at least show their respect officially in the international arena. Non-state actors are often out of any control by any

[17] BASTL, Martin, Gruberová, Zuzana. Cyberspace as a "Fifth Domain"?. In: *Vojenské rozhledy*, 2013, Vol. 22 (54), No. 4, pp. 10-21, ISSN 1210-3292. Available at: www.vojenskerozhledy.cz
[18] MINÁRIK, Tomáš. NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. In: *NATO CCDCOE* [on-line]. [cit. 2022–11–03]. Available at: https://tinyurl.com/2yeepu27
[19] *Warsaw Summit Communiqué* [online]. 2016. [cit. 2022-08-30]. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm
[20] *The Czech Armed Forces Development Concept 2030*. Prague: Ministry of Defence of the Czech Republic. 2019. pp. 15-19. Available also at: https://tinyurl.com/3mymdmaf

specific state or they can be used as proxies to perform specific tasks which states do not want to be associated with.

Even a perpetrator of offensive cyber activities (cyber operations, cyberattack, in further text just cyberattacks), in an effort to increase the effectiveness of their attack, e.g., distributed denial-of-service (DDoS) kind of attack, very often exploits many other computers in many countries world-wide, remotely controlled as "zombies". Owners of these misused computers, many times from allied or neutral countries, need not be aware that their hardware has become a part of such a cyberattack.

Uncertainty concerning the originator and also the executors of the attack may cause a challenge in bringing them to accountability and any rash reaction might be counterproductive.

Consequences of massive cyberattack on critical CIS infrastructure may block proper use of the cyberspace which may badly affect economies of states, medical and rescue systems, and supply systems and it may even lead to social unrest and threaten governmental control over the country. In general, this attack may decrease defence capabilities of the country by reducing the capability of its forces being strongly dependable on cyberspace. In total, the well-orchestrated cyberattack may cause consequences similar to a small or medium size armed conflict. On the other hand, not all offensive actions are necessary recognised as offensive operations, in many cases, small scale, not well-orchestrated individual activities with different intents may exist.

Cyberattacks organised by individuals or groups, regardless of their motivation, are discovered daily and even such attacks that are identified as state organised need not be necessarily part of war in the traditional meaning. They may be components of hybrid, below-threshold influencing operations, possibly accompanying an armed conflict. Moreover, Uppsala Conflict Data Program's categorisation of armed conflicts[21] is mainly based on numbers of fatalities, which need not be a direct consequence of a cyberattack. Labelling all cyberattacks as cyber war is in contradiction with the generally understood meaning of the term "war", i.e., a series of orchestrated campaigns, offensive and defensive operations containing appropriate actions, including attacks. Therefore, war is supposed to last longer than individual attacks.

Today, cyberattacks allegedly or really organised by states are parts of their attempts to influence opposing or hostile states in peace-time (e.g., Iran,[22] Estonia,[23] USA[24]) or within

[21] Upsalla Universitet. *UCDP Methodology*. [on-line]. n.d. [cit. 2022–11–05]. Available at: https://www.pcr.uu.se/research/ucdp/methodology/
[22] HOLLOWAY, Michael. Stuxnet Worm Attack on Iranian Nuclear Facilities. In: *PH241* [on-line] 2015. [cit. 2022–11–07]. Available at: https://tinyurl.com/59zkn3yh
[23] OTTIS, Rain. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. [on-line]. 2008. [cit. 2022–11–04]. Available at: https://tinyurl.com/2duvmp7n
[24] America is under cyber attack: why urgent action is needed. In: House Hearing, 112 Congress [on-line] 2012. [cit. 2022–11–07]. Available at: https://tinyurl.com/9z63z5u9

the already mentioned hybrid conflicts and certainly parts of real armed conflicts (e.g., Georgia,[25] Syria,[26] Ukraine[27]).

Due to the fact that except for *regular states* having responsibility for their citizens, there are and will be much more *non-state actors*, who are responsible just to their owners, having the capability to affect seriously national, regional and even global economy. In future, governments of states will be forced to decrease potential threats coming from cyberattacks organised by state and/or non-state actors to their economies to acceptable minimum, similarly to what Ronald Reagan and Mikhail Gorbachev did in the 1980s, still maintaining the capability to attack the enemy in this relatively new domain of combat activities but minimising the threats of its misuse.

Treaties or conventions prohibiting or strictly limiting offensive capabilities owned by non-state actors and commercial organisations are inevitable part of this agreement. It is also necessary to monitor all activities having symptoms of a certain level of a cyberattack as well as their originators in order to predict these attacks and ideally to prevent the originators to launch cyberattacks of any level.

It is a clear fact that all advanced users have potentially the possibility to prepare and launch a cyberattack, still, a great majority of them have no intent to do so. There always will be some communities of hackers, recruited from among young people, testing their abilities together with a level of protection of the most interesting networks and websites. There always will be criminally motivated perpetrators trying to obtain some personal profit and as well as people trying to fight against governments and the whole society due to their ideological, political, or religious orientation. It is possible to reduce two of the three mentioned groups in the long time horizon.

Online defence against any viruses, Trojan horses, or any malicious software of all computers will be an obvious part of internet communication provided by servers not allowing remote control of infected computers connected to server. Another protective measure might consist in the monitoring of activities aimed at carrying out cyberattacks and their automatic blocking.

Certainly, states will hold cyber capabilities in their inventories, both defensive as well offensive in their nature, as a tool of their sovereignty, like other branches of the armed forces' capabilities. However, having in mind that all states are able to substantially reduce the effectiveness of the use of cyber domain over a concrete territory with strong effect on the economy of others, they might agree on a scale of offensive actions in the cyber domain and adequate defensive actions in any domain. The goal is, on one hand, to reduce possible escalation and to increase transparency and predictability, on the other hand, to minimize the economic, social as well as political impact of such actions when they appear accidentally, contrary to the state's interests. Another thing states

[25] *Georgia-Russia conflict (2008)*. [on-line]. 2021. [cit. 2022-11-04]. Available at: https://cyberlaw.ccdcoe.org/wiki/Georgia-Russia_conflict_(2008)
[26] TODD, Brian, Brown, Forrest. Syria's cyberattack: First wave of a bigger war? In: *CNN* [on-line] 2013. [cit. 2022-11-07]. Available at: https://tinyurl.com/rmhhbvc9
[27] PRZETACZNIK, Jakub, Tarpova, Simona. In: *EPRS/European Parliamentary Research Service* [on-line] 2022. [cit. 2022-11-06]. Available at: https://tinyurl.com/mtyt4j6t

might agree on is the minimization of threats in cyber domain originated from non-state actors.

Comparing to the philosophy of non-proliferation policy in terms of controlling all storage factories, sites and institutions related to weapons of mass destruction, their dangerous components or double-use materials, in the case of cyber domain, it is not possible to monitor all computers as potential sources of a cyberattack of any kind. But there is a possibility and necessity to monitor all individuals already presenting their practical abilities and their intent to use them against the state. This is similar to incurable infectious carriers, which are potentially dangerous but it is not possible to neutralise them in democratic society. There is a legal possibility to keep them out of any computer, GSM, or other device with any access to the internet as proven in the U.S.A. by the court decision within last decades.[28]

CYBERSPACE AND LEGAL ASPECTS

The exploitation of domains must be complemented with protective measures of their lawful use. In accordance with rising threats, legality of offensive actions against infected, remotely controlled computers used during attacks on sensitive networks with fatal consequences, must be assured. What is the level of responsibility of the owners or users of these computers or providers of related services? Also, in this domain, the rule of law *ownership entails obligations* must apply, as stated, e.g., in Article 11 of the *Charter of Fundamental Rights and Freedoms*, which is a part of the constitutional order of the Czech Republic.[29] This regime is supplemented at the state level by the obligation to utilize due diligence principles. The state should effectively exercise their sovereign power and prevent (or punish) wrongful acts originated in its sphere and targeting other states or their subjects, as *The Unwilling or Unable Doctrine* implies.[30] Absolute protection in the cyberspace is a "bridge too far" and in real social and resource conditions it is almost unreachable, therefore, a holistic and permanent research together with the ongoing development of new methods is necessary. Certainly, owners have their level of responsibility, often their computers are not sufficiently protected to avoid their misuse, but may this fact be taken as a "casus belli", a reason for military action as defined in the *U.S. International Strategy for Cyberspace*?[31]

[28] BIDDLE, Sam. Infamous 15-Year Old Hacker Banned from Internet for Six Years. In: *GIZMODO*. [on-line] 2012. [cit. 2022–11–02]. Available at: https://tinyurl.com/44amh5fu
[29] *Constitutional act No. 2/1993 Coll., the Charter of Fundamental Rights and Freedoms*. Art. 11, par. 3. [on-line]. n.d. [cit. 2022–10–27]. Available at: https://tinyurl.com/mr23et8h
[30] HOLMQVIST SKANTZ, Madeline. *The Unwilling or Unable Doctrine - The Right to Use Extraterritorial Self-Defense Against Non-State Actors.* [on-line]. 2017. [cit. 2022–11–03]. Available at: https://tinyurl.com/2p8umvut
[31] *International Strategy for Cyberspace*. The White House [on-line] 2011. [cit. 2022–08–20]. Available at: https://tinyurl.com/2p963yzb

Cyberwar/Cyber warfare

In this context, the term cyberwar, sometimes called also cyber warfare, is used in connection with waging war activities in the cyberspace domain.

Nowadays, cyberwar is considered as part of hybrid or non-linear war. This classification is supported by Weissmann, who includes the cyber sphere in his seven dimensions of hybrid threats and hybrid warfare.[32] The term "non-linear war" is mentioned in Valery Gerasimov's article *The Value of Science in Foresight*.[33]

One of the first mentions of the term cyberwar appeared in the 1990s, in the publication by John Arquill and David Ronfeldt *Cyberwar Is Coming!*[34]

Professor John B. Sheldon[35] defines cyberwar as

> *"War conducted in and from computers and the networks connecting them, waged by states or their proxies against other states. Cyberwar is usually waged against government and military networks in order to disrupt, destroy, or deny their use."*[36]

Cyberwar, according to Sheldon, should not be confused with terrorist activities in cyberspace or cyber espionage or cybercrime. Although all of the above activities use similar tactics, it would be wrong to consider them all as cyber war.[37] Cybercrime represents *"the use of computer as an instrument to further illegal ends."*[38]

In the context of thinking about cyberwar as a new type of warfare, the question of the need for *offensive cyber capabilities* is often considered. If, from the point of view of the Armed Forces of the Czech Republic, we are concerned with assessing whether it is necessary to build offensive capabilities in the cyber domain or not, we can proceed from the *Security Strategy of the Czech Republic*, in which the strategic interest of the Czech Republic is declared to ensure the cyber security and defence of the Czech Republic.[39]

Given the current and anticipated development in the cyber domain, it is necessary that the armies of the North Atlantic Treaty Organization are not only prepared for cyberattacks, but above all that they also build their offensive capabilities in this domain,

---

[32] WEISSMANN, Mikael. "Conceptualizing and countering hybrid threats and hybrid warfare." *Hybrid Warfare*, London: Bloomsbury Publishing, 2021-61-82. https://doi.org/10.5040/9781788317795.0011.

[33] GERASIMOV, Valery. Tsennost nauki v predvidenii. *Voyenno-promyshlennyy kuryer* [online]. Moscow, 2013, 8 (476), 12 [cit. 2022-09-06]. Available at: https://tinyurl.com/3e8382d8

[34] ARQUILLA, John, David F. Ronfeldt. *In Athena's camp: preparing for conflict in the information age*. Santa Monica, Calif.: Rand, 1997. ISBN 0-8330-2514-7. p. 30.

[35] Professor of space security and cybersecurity, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama, U.S.

[36] SHELDON, John. B. Cyberwar [online]. [cit. 2022-08-29]. Available at: https://www.britannica.com/topic/cyberwar

[37] Ibid.

[38] Cybercrime. *Britannica* [on-line]. n.d. [cit. 2022-09-01]. Available at: https://www.britannica.com/topic/cybercrime

[39] *Security Strategy of the Czech Republic 2015*. Prague: Ministry of Foreign Affairs of the Czech Republic. 2015. ISBN 978-80-7441-005-5. Art. 14. Available also at: https://tinyurl.com/3sy5fyad

especially in a situation where Russia and China base their cyber activities on offensive state-security doctrine.[40] Adequate tools are also required for the possible activation of Article 5 of the Washington Treaty in the context of a cyberattack.

Cyberwar versus armed conflict

When looking at this issue from the perspective of international law, it is needed to address the meaning of the term *armed conflict*. Armed conflict is usually understood in two concepts, namely international armed conflict and internal armed conflict, differing subjects or territories.

For the purposes of this article, the concept of armed conflict is defined as an international armed conflict. By this term, however, both the traditional war conflict between two or more states are understood, regardless of its declaration, and liberation wars against foreign occupation, colonial powers, or racist regimes.[41] In the scope of this work, the armed conflict is perceived primarily from the point of view of the traditional war conflict.

Traditional armed conflict is characterized primarily by the fact that it is bound by the norms of international humanitarian law, of which the *Geneva Conventions* and related documents play a pivotal role. These standards, among other things, define the concept of a combatant and quite strictly determine their features, in particular, distinguishing them from other subjects[42]. Conventional ways of fighting thus have their own rules and it is clear or identifiable which side is fighting against the other.

Unlike a traditional armed conflict, cyber war takes place in a virtual world without the possibility of clearly identifying the adversary, which may cause a challenge to bring perpetrators to justice. In this anonymous sphere, it is not possible to define unequivocally that this is an attack by a particular state. In a majority of cases of such attacks, it will not be a cyberattack as a part of war conflict but a crime committed by individuals or by organised groups not following political or military goals. These examples belong to the "grey zone" of the existing legislation.[43] Although advanced societies have the technical means to accurately detect the place or unit from which the cyberattack was conducted, there is no guarantee that such an act was committed by a person who is located on the site or owns the device from which the attack was conducted, since there is a possibility, or let us say a high probability, that the device was subjected to hacking activities, precisely in order to divert the trace from the real actor.

Another problem that makes it difficult to distinguish whether it is an act of war or "only" a criminal act is in the person of the executor or offender. If the person does not admit a connection between the attack and the state and this connection is not proven to the state, it will not be an act of war, but the act will be considered from the point of view of the criminal liability of either an individual or a group of persons. However, if a state

[40] *The Czech Armed Forces Development Concept 2030*, ref. 19, p. 13.
[41] FUCHS, Jiří. *International Humanitarian Law*. Prague: Ministry of Defence of the Czech Republic. 2007, pp. 26-28. ISBN 978-80-7278-424-0.
[42] *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts*, June 8, 1977, 1125 U.N.T.S. 3. Art. 43-44
[43] ŠTRUCL, Damjan. Comparative study on the cyber defence of NATO Member States. In: *NATO CCDCOE* [on-line]. 2021. [cit. 2022–11–03]. Available at: https://tinyurl.com/k4vcyxnt

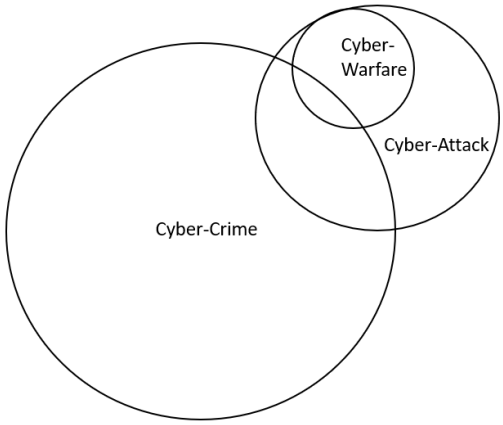
declares that a cyberattack was conducted against another state with the intention of using force and means against the other state, this attack will be viewed from the point of view of the law of war.

A state will always bear international legal responsibility for cyber operations that are attributed to it and that constitute a violation of international law as is stated in Rule 6 of the *Tallinn Manual*.[44]

Interesting is the consideration of the possible activation of Article 5 of the *Washington Treaty*[45] in connection with a cyberattack. It is known that the North Atlantic Treaty Organization is based on the principle of collective defence and military cooperation.[46] Problematic in this case will be the assessment whether to subordinate the attack to the act of war or not, as we have already discussed above. However, there is no doubt that if such an attack was carried out, for example, against state sovereignty, territorial integrity, population, critical infrastructure by the will of a foreign state, there would be a legal basis for the application of this provision.

Figure 2: Cyber actions and their characteristics

Relations between cyber action



Essential characterisistics of different cyber actions

Type of Cyber-Action	Involves only non-state actors	Must be violation of criminal law, committed by means of a computer system	Objective must be to undermine the function of a computer network	Must have a political or national security purpose	Effects must be equivalent to an "armed attack", or activity must occur in the context of armed conflict
Cyber-Attack			√	√	
Cyber-Crime	√	√			
Cyber-Warfare			√	√	√

Reproduced by the authors. Source: HATHAWAY, Oona A. et al. *The Law of Cyber-Attack*. California Law Review [on-line]. 2012, vol. 100, no. 4, p. 833. [cit. 2022-08-03]. Available at: https://www.californialawreview.org/print/2the-law-of-cyber-attack/

[44] *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. 2013. ISBN 978-1-107-02443-4. p. 29. Available also at: https://issuu.com/nato_ccd_coe/docs/tallinnmanual

[45] *The North Atlantic Treaty*. Washington [on-line]. 1949. [cit. 2022-09-11]. Available at: https://www.nato.int/cps/en/natolive/official_texts_17120.htm

[46] Ibid. Art. 3, 5

CONCLUSION

There is no real hope that attempts to launch attacks in the cyber domain by states, non-state actors, or individuals in peace-time will be stopped. There will always be young people trying their abilities in cyberspace out of inborn curiosity; this will offer a possibility for the state to recruit new experts for its cyberspace organisations. Also, there will always be criminals in illegal groups or individuals trying to gain illegal economic or political profit or support for their goals.

It is in the interest of states and international community to control traffic in the cyberspace and to suppress or at least to reduce all illegal activities in this domain, while respecting fundamental human rights and freedoms. States can exercise their tools, legislation, and state organised legal power together with the legitimacy of such state-controlled activities. A part of actors in the cyberspace are international, non-state organisations, also having their interests in this domain, still, with no legality or legitimacy to organise offensive actions on their side. Only the protection of their systems might be considered legal, using the same legality as any other private persons. Offensive actions have to be declared as only state-owned measures, just like any other offensive military measures.

Signed international treaties and conventions have to create such legal environment that would enable full control of any offensive or double purpose capabilities of non-state actors as it has already been used in the case of weapons of mass destruction together with their carriers, combat aircraft, attack helicopters, guided missiles of any range with warheads and more. There is at least one challenge to find a common denominator as a basis for the mentioned treaties; till today, majority of all legislation in this field is based on recommendations without direct obligations to accept them, esp. in the commercial sphere.

Unlike the legislation of the land, sea, air, and space domains, the cyber domain remains vulnerable so far. Although the North Atlantic Treaty Organization as well as the European Union try to react to the situation and to related cyber threats, as indicated in the *Strategic Compass*[47] and *NATO 2022 Strategic Concept*,[48] there is still no unitary worldwide binding regulation, e.g., at the United Nations level, governing activities in this area. This situation allows for chaotic exploitation, uncontrolled attacks, cybercrime activities on an international as well as on a national level. Given that the cyber domain is used for the benefit of all other domains, the impossibility of its full and at the same time safe use can lead to the blocking of the exploitation of the cyber domain, with a fundamental impact on activities in other domains. Failure to ensure the functionality of the cyber domain as global commons and allowing its possible abuse can have crucial effect on global security. Therefore, in this context, the possible application of the M.A.D. concept is increasingly being referred to.

[47] *A Strategic Compass for Security and Defence for a European Union that protects its citizens, values and interests and contributes to international peace and security*. Brussels: Council of the European Union, 7371/22. 2022.
[48] *NATO 2022 Strategic Concept*. NATO. 2022.