Hadtudományi Szemle
14. évfolyam (2021) 4. szám 5–16. • DOI: 10.32563/HSZ.2021.4.1

Kristóf Kralovánszky[1]

Certain Connections between Cyber Operations, Artificial Intelligence and Operational Domains

Abstract

The relationship of operational domains with various systems based on artificial intelligence is becoming more profound and more diverse. The ability to influence decision-making mechanisms can pose serious risks that need to be identified and interpreted. Cyberspace is the carrier of artificial intelligence, but the latter as an operational domain has not yet been identified. The goal of this study is to examine certain relationships between cyberspace, artificial intelligence, and operational domains from a state-will enforcement perspective, using mostly qualitative tools, combined with quantitative elements. As a result, this paper finds the need to review defence doctrines from a cyber operational perspective and suggests addressing artificial intelligence in a much broader context, especially in the defence and military contexts.

Keywords: *cyberspace, military domains, artificial intelligence, critical infrastructures*

1. Introduction

Discussing technical subjects from a military science (not engineering) perspective might seem like a contradiction in terms. To a specific aspect, it is, but above a particular level, the two separate threads (science and engineering) must come together and strengthen each other. Taking cyber operations and cyberspace as an example, such consolidations evolve to become policy. In many cases, strategy can remain below the radar,[2] mostly for operational safety reasons – which is the case in most cyber operations.

According to Clausewitz, war itself is an instrument for political act.[3] If we generalise this principle, we can safely say that military operations are the same instruments, but

[1] University of Public Service, Doctoral School of Military Engineering, PhD student; University of Public Service, Department of Electronic Warfare, junior Assistant Professor; e-mail: kralovanszky.kristof@uni-nke.hu

[2] Such strategies do exist but are highly classified, so the result is that they are not visible for the public eye.

[3] Carl von Clausewitz, *A háborúról* (Budapest: Zrínyi Kiadó, 2014).

possibly on a lower level. However, if we look back to the 19th century, there were only two domains that an armed force could use: land and sea. In that sense, Clausewitz's thinking was limited to those two areas.

The 20th century brought a new domain: the air force. The 21st century (and only 21 years have passed from it) already brought two new domains: cyber and space.[4] The force behind a political act remains unchanged: states wishing to pursue and enforce their interests to achieve the best possible position within a region or in the system of certain states.

2. Enforcement of State-will

It is essential to distinguish between political- and state-will enforcement. There is always a political will behind the enforcement of a state's will, but this special enforcement is typically only possible by a political force with state authorities and power. It is possible that in domestic politics, a given party or organisation has a serious political weight (in fact, it may even be in the majority), but it is still incapable of enforcing its will at the state level. This study further interprets political will as the motivation behind state-will enforcement.

In most cases, enforcing one's will seeks to make optimal use of its resources, but at the same time, politics very often mixes emotions into its actions. This is part of the reason why many state-run operations are not (always) rational.[5]

In each case, a state seeks to assert its own will and achieve its own goals – but it does so in a dynamically changing international environment in which power relations are also constantly changing. As a result, it will at all times strive to achieve the best position in a given situation and, in many cases, afford a partial violation of the sovereignty of other states, since sovereignty is not an absolute concept and its interpretation follows changes in the political environment in the same way.[6]

This logic is perfectly valid for cyber operations as well, as state (subsidised) enforcement is precisely the same will. As with all military operations, all state operations will evaluate targets and designate assets once targets have been identified. Even in this process, there can be a kind of goal, since the use of a particular tool can be of message value in itself.[7]

The growth of cyber operations is primarily due to their efficiency and excellent price/value ratio. However, they would be almost entirely worthless by themselves, as it is impossible to occupy physical space with cyber operations. Therefore, a suitable

[4] Space could be considered an older domain in a military context as well, considering that President Ronald Reagan announced the Strategic Defense Initiative in 1983. This program was meant to be of defensive nature only and considered attacks initiated from the air, land or sea and not from space. From a definition perspective, a domain can be used to initiate, perform and conclude an armed conflict in that same domain.

[5] Emotions and rational decisions usually do not mix. In an ideal scenario, a state action's outcome is carefully calculated, however, strong emotions can easily override such calculations. The strength of emotions and the level of override can be in direct proportion.

[6] Gergely Varga, 'A vesztfáliai szuverenitás érvényessége a nemzetközi kapcsolatokban', *Nemzet és Biztonság* 8, no 1 (2015), 30–38.

[7] A kinetic detonation, as a response, can be carried out in several ways: with a missile, an explosive deployed on the ground, a suicide bomber. The method can also be interpreted as a reference to the defendant.

target is also needed for cyber operations to work. Humankind has created more and more vulnerabilities in its own environment, and one of the best examples of this is the system of critical infrastructures.[8]

In offensive cyber operations, the use of conventional armed force has become partly redundant, as the operation itself requires intelligence (i.e. information related to the systems to be attacked) and an appropriate IT system/knowledge.[9] This may very well be available to the armed forces, but any state-aided organisation may also be able to carry out the operation, as it does not require a weapon in the classical sense and the logistical background that serves it.[10]

The smooth operation of critical infrastructures, including the continuous and stable operation of their interdependencies, is a precondition for the stability of a country. Thus, failures of some critical components (whether in the same or a different sector) for weeks or more will alone result in almost guaranteed instability, both in economic and domestic terms.[11] This is mainly why the target value of critical infrastructures is exceptionally high from an attacker's perspective.

On the defence side, the armed forces of a given country are, in typical cases, unavoidable. In the case of a cyberattack, especially when targeting a critical infrastructure, the attacker's intention to do damage is clear and it is equally clear that they wanted to harm the attacked country as a whole. Therefore, from this point of view, it is not necessarily relevant whether kinetic destruction has occurred or whether anyone has lost their life. A threshold needs to be set beyond which an offensive cyber operation should be interpreted as an armed attack. However, pre-determining this threshold can be a serious problem, as it is difficult to generalise the damage caused by an unforeseen attack vector. It is also not practical to start with an itemised list of infrastructures and damages since it would give unnecessary ideas to a potential attacker. Determining the threshold is, therefore, a sensitive political issue for these reasons, as well.

Therefore, it can be concluded that state-will enforcement through cyber operations raises several critical questions related to defence doctrines that should be addressed quickly and effectively.

3. Artificial intelligence as a defining new area

It is important to discuss an exceptionally rapidly evolving area, which is increasingly becoming a determinant of our standard technologies: artificial intelligence (AI).[12]

[8] There have always been resources in societies whose targeted attacks could have caused severe damage. Such were wells (thousands of years ago), which were often poisoned by adversaries, thus severely limiting the access to potable water for those living there. It is equally true today that the infrastructures requiring the highest level of protection are drinking water reservoirs and drinking water distribution systems.

[9] This summary might be an oversimplification, but in its true essence, it reflects reality. Obviously, the armed forces' own intelligence background (also) may already be a condition for obtaining credible and actionable intelligence.

[10] Jori Pascal Kalkman and Lotte Wieskamp, 'Cyber Intelligence Networks: A Typology', *The International Journal of Intelligence, Security, and Public Affairs* 21, no 1 (2019), 4–24.

[11] László Kovács, *A kibertér védelme* (Budapest: Dialóg Campus Kiadó, 2018).

[12] Peter Layton, 'Fighting Artificial Intelligence Battles. Operational Concepts for Future AI-Enabled Wars', Centre for Defence Research, Australian Defence College, *Joint Studies Paper Series,* No. 4.

It will be confirmed or refuted in the coming years, but AI is increasingly beginning to have domain-like characteristics. However, to better understand this, we need to look back at earlier stages of electronic warfare. Even before cyberspace and cyber operations, there were computers, there were computer networks that our society actively used. They were parts of everyday life – especially in the economic and military spheres. As time went by, their importance grew, their field of application widened, and they started to play a decisive role in the functioning of society.[13]

Regarding their components, we are talking about electronic devices that existed before, but their development has significantly increased their processing speed and wide availability. Examining the development of similar properties of AI, we find precisely the same thing. AI is based on computer systems, just as computer systems were based on electronic devices. Self-propelled (sub) AI systems are now part of every new smartphone on the market. Almost all new (up-to-date) desktop operating systems already have machine learning systems. Such are the built-in firewalls and intrusion protection systems. Based on our web browsing, various AI systems deliver customised advertisements to us. Our electronic mail systems also perform SPAM filtering using AI-based algorithms.

However, one of the most significant differences is that with proper hardware, it is only a matter of software if AI is present or not. In other words, if the appropriate hardware is available, an AI system can be installed on the hardware without needing to replace additional hardware. The direct consequence of this is that an AI system can be upgraded through software only, which provides additional capabilities or greater efficiency. To achieve the same in the past, parts had to be replaced in an electronic system or a new machine had to be purchased.

Behind the modern analytic tasks, we will find AI-supported systems in almost all cases. The kind of spread that was visible between the birth of electronic devices and cyberspace can be observed between cyberspace and AI systems. However, there is another significant parallel. Cyberspace cannot be interpreted and is dysfunctional without infocommunication systems. The same is true for AI systems: they are inoperable without infocommunication foundations. But there is a crucial difference. By definition, a computer alone (without network connections) is not part of cyberspace. An AI system (when properly configured) can work on its own. This, of course, requires that the AI system be loaded with the right amount and quality of data and have a local user interface. If these are available, the AI system can answer the question (posted) defined in the user interface. At the same time, isolation also means that the decision-making process will be based only on the stored data – although under certain circumstances, this decision-making database can be updated manually (e.g. via USB drive).

In a holistic view, cyberspace is a vital element of all military domains,[14] AI is rapidly starting to behave very similarly.

[13] Négyesi Imre, 'A mesterséges intelligencia katonai felhasználásának társadalmi kérdései', *Honvédségi Szemle* 149, no 1 (2021), 133–144.

[14] Jared Donnelly and Jon Farley, *Defining the 'Domain' in Multi-Domain* (Joint Air Power Competence Centre, 2019).

4. Possible risks of AI systems

Based on the above, the operation of AI systems should be divided into two parts: distinguished between networked and non-networked AI systems.[15] One crucial question is whether a non-networked AI system could pose a risk to the operator (organisation) or to the country of operation? The answer is a resounding yes, as it may be able to make autonomous decisions independently of the network. From a different perspective, the risk lies not only in network availability but also in decision-making and its use.

Going further on this idea, it is necessary to examine how the risks of decision-making can develop? AI systems, like all infocommunication systems, consist of at least one hardware and one software component. The operation of the software part is based on the standard operation of the hardware elements. However, an individually modified, unique hardware device can implement the standard operation and, at the same time, additional functionality according to the will of the modifier. So it is possible to create hardware that matches the traditional version in all respects (in appearance, design and basic operation) and has additional capabilities. A simple example of this is a phone charging cable that incorporates a miniature web server and data logger.[16] It looks virtually indistinguishable from a traditional, factory-charged charging cable, but it gives its installer (partially) free access to the phone they charge, so an attacker can easily learn about the data stored on the device.[17]

A software-based attack on an AI system can also work without a network connection. During the development of the AI system, backdoors can be created, which are known only to the developer and remain hidden from the user (operator). Through such a backdoor, not only data can be extracted from the system, but new data can be recorded or the decision-making process can be modified. During the learning process, intentional mistakes are possible where a recognised object is associated with the name of another object, i.e. an "apple" will be treated as a "lemon" or a "chair". The risks involved are almost self-evident.[18]

A similar problem is when an AI system judges incorrect behaviours to be correct and vice versa. A good example of this problem was in 2016, when an AI-based chatbot developed by Microsoft called Tay, was launched as a sociological experiment by its creators (otherwise intended for entertainment).[19] The app should have picked up the style of a 19-year-old, but as part of that, he very soon began sending extremely racist and inciting messages. Those who communicated with Tay soon realised how it was possible (and how easy it was) to teach him, and the bot was directed to Internet content from which he gained this blatantly extreme knowledge. Following serious community outrage, the manufacturer shut down Tay less than 24 hours after the

[15] The vast majority will be networked AI systems.
[16] See https://shop.hak5.org/products/o-mg-cable-usb-a
[17] The course of attack is much more complex, but the concept works in the real world with proven records.
[18] Paul Maxwell, *Artificial Intelligence Is the Future of Warfare (Just Not in the Way You Think)* (Modern War Institute, 2020).
[19] Rachel Metz, 'Microsoft's Neo-Nazi Sexbot Was a Great Lesson for Makers of AI Assistants', *MIT Technology Review,* 27 March 2018.

start.[20] Such flaws were more common 3–4 years ago, but manufacturers were quick to respond, and similar fundamental problems became rare. It can also be considered a development curve which is now in the past. However, technology evolved to the next level, and flaws of similar sizes are a lot more challenging to pinpoint.

5. AI systems built on each other

Likewise, the risk of manipulating a voice recognition and dictation system can be extremely high. The software itself recognises the voice of the given (logged in) user and describes it in the text field of an application. If the application is not operated by the initial user, the recognition will start to be distorted and after a few hours the voice recognition of the original user will start to fail. In a critical case, the adaptation of the original user may be so distorted that it becomes necessary to delete it. The audio adaptation file of the same system, which contains the recognition dictionary, can be attacked, for example, the word "left" can be changed to "right", which can be a severe problem in a medical application. In this case, the system recognises the word "left" and then describes it as "right" according to the dictionary.

The former example is very thought-provoking given that the number of (mobile) devices running an application with voice recognition functionality is expected to be around 7–8 billion by the end of 2021, meaning that on average, such a device will reach every inhabitant of the Earth.[21] An additional risk is that apart from similar applications available only in the Chinese domestic market, this value is shared by five manufacturers: Apple Siri, Google Assistant, Microsoft Cortana, Amazon Alexa, Samsung Bixby.

One of the most spectacular appearance and (accessible to anyone with internet connection) is the appearance of "deepfake" technology. It is able to montage a user-narrated text from a few photographs[22] of an existing person to that person, resulting in any text that can be told by a freely chosen person. There is an amateur version of this software that can be downloaded to a smartphone, with limited characters and basic videos, so its fake is relatively noticeable.[23] A professional solution to this can also be found as early as 2017, from scientific research and development at Washington State University.[24] The authenticity of videos of this quality can often only be established by secondary means or indirectly – using highly sophisticated analytic and forensic technology.

AI systems as mentioned earlier can be extremely complex, which also means that they involve interdependent decision-making. That is, they have separate AI subsystems operating on several levels, where the output of one AI subsystem becomes the input of the subsequent system. If there is no comprehensive control (in the received data/

[20] Paul Mason, 'The Racist Hijacking of Microsoft's Chatbot Shows How the Internet Teems with Hate', *The Guardian,* 29 March 2016.

[21] Sandra Vogel, 'More Digital Assistants than People by 2021 Says Ovum', *Internet of Business,* 15 July 2021.

[22] Using only a few photos will not result in totally lifelike appearance, however, the teaching of hundreds of images from different angles will considerably improve the quality of the forged footage.

[23] Jon Porter, 'Another convincing deepfake app goes viral prompting immediate privacy backlash', *The Verge,* 02 September 2019.

[24] Jennifer Langston, 'Lip-Syncing Obama: New Tools Turn Audio Clips into Realistic Video', *UW News,* 11 July 2017.

information) between the interconnected systems, an additional risk (and possibility of attack) appears. This is because it becomes unnecessary for the attacker to get to know and manipulate the AI algorithm in detail. It is sufficient to attack transitions between subsystems and inject a data set desired by the attacker as the data input of a higher system. If this is accepted as authentic by the higher system, the attack is successful and the attacker achieved the goal of influencing.

In the case of newer surveillance cameras (used both for civilian and military purposes), the primary processing of AI takes place in the camera, which a few years ago was only possible on the server side due to the high CPU performance demand. This technological step also allows for the mass spread of facial and behavioural recognition technologies (systems). However, examining the risk side, autonomous decision-making at the law enforcement level appears, a closer observation of a person can begin – based on an AI system's evaluation. Ideally, this poses no risk to the observed individual since recordings of him or her will be deleted after a specified (and relatively short) period of time. The problem is much more serious when statistics records the fact of observation without stating that such observation was unjustified and was without true cause. It may be that a person actually needs to be monitored once, but system statistics will show that they have already been monitored four times – but each time this was due to an error in the AI's decision.[25]

Facial recognition and, more broadly, biometric identification are increasingly popular and relatively widely accepted authentication methods. It has now been proven that their reliability is far from being as high as manufacturers or implementers want it to be. It is also true that the biometric part itself – that is, the iris, the 3D portrait, the vein, etc. – is difficult to falsify, but the procedure has an intermediate step: where the read data is compared with the data stored in the databases. This is because the originally uploaded face image can be modified by uploading a properly prepared duplicate so that it can be identified as another person during the comparison. The novelty of this type of attack is that it is not necessary to know the internal AI algorithms of the facial recognition system for this deception.[26]

Basic AI implementations can be found in numerous military applications, similar to civilian use: semi-autonomous vehicles, robots and biometric recognition.[27] One precious and specific military use is in multisource intelligence evaluation, especially in a combat/tactical environment. Deep descriptions of such systems in unclassified documents are scarce. These are good warnings that widespread new technology in crucial systems can be problematic without proper (real world) experience. The use of such technologies in crucial systems[28] without extensive field testing can be dangerous. Finding the right balance between test-times and speedy implementation can be a true challenge.

[25] Kristóf Kralovánszky, 'A kibertér fejlődése', *Hadmérnök* 14, no 4 (2019), 197–212.

[26] See https://adversa.ai/report-secure-and-trusted-ai/

[27] Adriana Gibson, Andrew J Merchant and Brandon D Vigneron, 'Autonomous Systems in the Combat Environment: The Key or the Curse to the U.S.', *The Strategy Bridge,* 08 October 2020.

[28] Especially in military identification/authentication processes.

6. Autonomous decision-making

A much more serious dilemma is when the use of lethal force (as a design goal) becomes possible based on the decision of AI systems. In March 2020, a Turkish STM Kargu-2 4-rotor drone[29] caused the death of an individual in Libya.[30] This drone is programmed to be able to identify targets even in the event of loss of communication with the controller and destroy such target after positive identification. That is, there does not necessarily have to be operator approval between the identification and the destruction stages. This particular type of drone destroys the target in such a way that an explosive device is mounted on it, and the aerial vehicle guides itself to the target at maximum speed. This, of course, destroys the drone itself as well, but even so, the aircraft part is extremely cheap, as it is worth only a few thousand Euros (excluding the warhead). And once destroyed, the same controller will control the next, new drone.[31]

The above technology can, of course, be extrapolated since it does not matter to the software whether it guides a drone onto the target, or it does the same with a rocket with greater destructive power in the classical sense. The more important question is the moral part: can we allow for human life to be extinguished fully autonomously, without a human decision?[32] It can be argued that by launching the drone, such decision was already made, as such possibility was considered. The problem with this reasoning is that the possibility of error in the decision process (due to software error or the hacking of the software) cannot be considered. In specific scenarios, it can be called collateral damage, but the moral essence remains highly questionable.

The possibility of interfering in the decision-making process should also be examined here, that is, the question must be asked: what is the risk from cyberspace of a partially autonomous weapon whose handler is not in direct and guaranteed closed (and secure) connection with the weapon? The simple answer is that if the connection itself (between the weapon and the operator) can be attacked and/or the control, arming or detonation is based on partial software (non-mechanical) methods, then the weapon can be attacked. The success of such an attack strongly depends on the complexity of the communication systems/software. Thus, the assessing of such vulnerability must consider the knowledge and experience required for a successful attack.

It is also an open question that if there is death resulting from the operation of an AI system, who has legal responsibility? An example is the 2017 accident[33] of a Tesla Model X, in which the vehicle's partially self-driving system[34] drove the vehicle into a reinforced concrete track separator at a speed of 110 km/h with virtually no braking.[35] The accident investigation found that there were several faults in the

[29] See www.stm.com.tr/en/kargu-autonomous-tactical-multi-rotor-attack-uav

[30] United Nations, *Final report of the Panel of Experts on Libya established pursuant to Security Council Resolution 1973 (2011), Pub. L. No. S/2021/229.*

[31] For the sake of thought, it is worth addressing the question of what would happen if such drones were used not in themselves but in autonomous swarms.

[32] This paper does not intend to examine the answer to the question posed in part, nor does the question itself belong primarily to the field of military science.

[33] Following the accident, the driver of the car died due to extreme forces in the collision.

[34] Tesla calls this system "AutoPilot".

[35] Rebecca Heilweil, 'Tesla Needs to Fix Its Deadly Autopilot Problem', *Vox,* 26 February 2020.

semi-self-driving system, but in legal terms, the manufacturer never claimed that the vehicle was capable of driving fully automatically without a driver. Moreover, the manufacturer explicitly warned that the driver of the vehicle must be able to intervene at any time to manoeuvre, accelerate or decelerate the vehicle.

7. Domains built on each other

The domains of military operations should also be examined from a perspective of subordination/superiority.

First, by examining the classical (land, water, air) domains, it can be concluded that land is a condition for the other two domains, since both sea and air operations require land – mainly to ensure the flawless operations of supply chains. Both marine vehicles and aircraft can transport food and fuel required for themselves and their crews. This self-supply is usually available for a period of a few hours to a few months, but sooner or later, land will be needed to replenish the stocks.[36]

Cyberspace, which is defined as the fourth domain, cannot be interpreted without infocommunication systems. Since infocommunication systems also rely very heavily on land (land-based) components, cyberspace's reliance on land cannot be questioned.

Space as the fifth domain is inoperable without cyberspace, as spacecraft orbiting in space require constant communication with terrestrial centres, especially to stay on orbit accurately.[37] As in space, autonomous vehicles are becoming more common in the sea and air domains. However, their autonomy is not yet absolute and in all cases they are equipped with communication capabilities that presume some kind of wireless network connection.[38] And if they have network connectivity, they are also, by definition, part of cyberspace.

It is clear, that without classical domains cyberspace cannot be interpreted, and without cyberspace, space (in its present form) is inoperable, meaning that a proper attack on classical domains can limit cyberspace and outer space capabilities. The reverse is also true, i.e. a stand-alone, well-targeted, and successful attack on cyberspace and space domains can significantly limit operational and civilian capabilities in traditional domains.[39] Cyber experts will argue that for a successful cyber operation, the conventional domains are not really required. In a narrow sense, they might be right; however, on a broader horizon, considering the land components of communications, the proper intelligence required for a successful operation all lead to a conclusion: control over land (as a domain) remains a requirement. From another approach, we can say that there are extremely strong interdependencies between land and cyber

[36] When examining cyberspace and AI systems, it is irrelevant which of the classical domains is considered the primary determinant, especially since the classical domain currently in use will be authoritative due to the duration of the execution of a cyber operation.

[37] If we examine the theory of offensive weapons deployed in outer space, communication is also necessary since launching an attack requires some kind of ground control (at least for orbit corrections).

[38] Such connection can be satellite-based, in older systems VLF (Very Low Frequency) can still be utilised.

[39] It is sufficient to attack the control system of navigation satellites (cyberspace) or the navigation satellites themselves (in space). Of course, such aggression will result in the most severe and immediate counterattack, so the attack clearly does not worth it. However, it does not change the logic of the basic operation of domains.

domains. The same remains valid for the connection between the cyber domain and AI. So in this context, AI also becomes interpretable as a domain-like realm, as similarly to cyberspace, independent processes can take place in AI. Such processes can have severe effects on other official domains.

The order of domains is listed in the chronology of NATO's adoption of cyberspace and outer space.[40] Other classifications, such as Ronald Fogelman's[41] system, designate space as the fourth and information operations as the fifth domain.[42] Without going into details, Fogelman's classification remains partially true considering information operations. However, the components thereof have considerably changed and cyber operations (in many cases) are fundamental elements of more comprehensive information operations. Today the proper nomenclature could be "information realm" (as opposed to "information operations") in a domain sense. The problem with "information realm" is that it is too broad and contains cyber, AI and computer network operations (which are now cyber operations). From a different perspective, the term "information domain" would be equal to "conventional domain" – containing land, air and sea. That would be an oversimplification of domains, which might not serve the purpose of reflecting actual reality in descriptions. Such a debate is also a prime example of how radical advances in technology during the course of 15–20 years can transform thinking about the fundamental domains of state-run, state-sponsored military/security operations.

8. Conclusion

For classical military science, the use of armed force and state-will enforcement are interdependent and separate areas. With the significant expansion of cyberspace as a domain and AI, state-will enforcement has received a new and broad set of tools, the use of which, especially on the offensive side, does not necessarily require the armed force of a given state.

As a result of operations in these domains, new risks have emerged that fundamentally threaten the functioning of a country, as attacks on critical infrastructures in that country can significantly and permanently limit economic, social processes and state governance.[43]

It would be important not only for technical and ethical studies to be conducted in the military application of AI, but also for its consideration to appear on a doctrinal level.[44] Interdependent decision-making processes, insofar as they are based on AI, are not merely man-made support systems but can have severe and autonomous

[40] NATO recognised cyberspace as an independent domain on 9 July 2016 at the Warsaw Summit. Space as a domain was recognised by NATO at the December 2019 meeting of Heads of State and Government.

[41] General, United States Air Force. Chief of Staff of the U.S. Air Force, 1994–1997.

[42] Ronald R Fogelman, 'The Fifth Dimension of Warfare', *Defense Issues* 10, no 47.

[43] Zsolt Haig and László Kovács, *Kritikus infrastruktúrák és kritikus információs infrastruktúrák* (Budapest: Nemzeti Közszolgálati Egyetem, 2012).

[44] Research concerning AI in the armed forces is extensively performed at the University of Public Service, Faculty of Military Science and Officer Training. Col. Haig and Col. Négyesi cover different aspects of this field and have numerous publications on the subject.

influence, even at the strategic level. In other words, strategic decisions can be made on information summarised solely by AI.

Advances in technology have demonstrated that we have gone well beyond the level where it is sufficient to deal with AI as a narrow part of information operations.[45] In the early 2000s, cyberspace was seen as a unique blend of information technology and cybernetics. It was not until 2016 that NATO accepted its existence at the Alliance level – while the same Alliance already established the Cyber Defence Centre of Excellence in Tallinn in 2008. For this centre to be established, Estonia had to suffer the consequences of the 2007 cyberattacks. Just as cyberspace has become an increasingly integrated part of our lives, AI is becoming the foundation of electronic decision-making systems. All of this happens by often considering AI just one of the smaller components of cyberspace or an advanced software.

The lifecycle of technical devices used in defence (especially AI-based systems) has been significantly reduced – mainly due to the commercially available and constantly evolving products and services available to adversaries. On the defence side, we are not necessarily talking about classical depreciation but rather about forced and technological obsolescence. This represents a major paradigm change and requires a fundamental shift in thinking on the design and procurement side. Therefore, responses to threats must necessarily follow the same innovation curve that appears on the attacker side. Losing out on the pace of development will widen the gap between the attacker and the defensive side, resulting in defects of defence capabilities and ultimately in partial incompetence.

References

Clausewitz, Carl von, *A háborúról.* Budapest: Zrínyi Kiadó, 2014.

Donnelly, Jared and Jon Farley, *Defining the 'Domain' in Multi-Domain.* Joint Air Power Competence Centre, 2019. Online: www.japcc.org/defining-the-domain-in-multi-domain/

Fogelman, Ronald R, 'The Fifth Dimension of Warfare'. *Defense Issues* 10, no 47. Online: www.hsdl.org/?abstract&did=439942

Gibson, Adriana, Andrew J Merchant and Brandon D Vigneron, 'Autonomous Systems in the Combat Environment: The Key or the Curse to the U.S'. *The Strategy Bridge,* 08 October 2020. Online: https://thestrategybridge.org/the-bridge/2020/10/8/autonomous-systems-in-the-combat-environment-the-key-or-the-curse-to-the-us

Haig, Zsolt and László Kovács, *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* Budapest: Nemzeti Közszolgálati Egyetem, 2012.

Heilweil, Rebecca, 'Tesla Needs to Fix Its Deadly Autopilot Problem'. *Vox,* 26 February 2020. Online: www.vox.com/recode/2020/2/26/21154502/tesla-autopilot-fatal-crashes

[45] David Vergun, 'Artificial Intelligence Key to Maintaining Military, Economic Advantages, Leaders Say', *U.S. Department of Defense News,* 09 April 2021.

Kalkman, Jori Pascal and Lotte Wieskamp, 'Cyber Intelligence Networks: A Typology'. *The International Journal of Intelligence, Security, and Public Affairs* 21, no 1 (2019), 4–24. Online: https://doi.org/10.1080/23800992.2019.1598092

Kovács, László, *A kibertér védelme.* Budapest: Dialóg Campus Kiadó, 2018. Online: https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf

Kralovánszky, Kristóf, 'A kibertér fejlődése'. *Hadmérnök* 14, no 4 (2019), 197–212. Online: https://doi.org/10.32567/hm.2019.4.13

Langston, Jennifer, 'Lip-Syncing Obama: New Tools Turn Audio Clips into Realistic Video'. *UW News,* 11 July 2017. Online: www.washington.edu/news/2017/07/11/lip-syncing-obama-new-tools-turn-audio-clips-into-realistic-video/

Layton, Peter, 'Fighting Artificial Intelligence Battles. Operational Concepts for Future AI-Enabled Wars', Centre for Defence Research, Australian Defence College, *Joint Studies Paper Series,* No. 4. Online: https://doi.org/10.51174/JPS.004

Mason, Paul, 'The Racist Hijacking of Microsoft's Chatbot Shows How the Internet Teems with Hate'. *The Guardian,* 29 March 2016. Online: www.theguardian.com/world/2016/mar/29/microsoft-tay-tweets-antisemitic-racism

Maxwell, Paul, *Artificial Intelligence Is the Future of Warfare (Just Not in the Way You Think).* Modern War Institute, 2020. Online: https://mwi.usma.edu/artificial-intelligence-future-warfare-just-not-way-think/

Metz, Rachel, 'Microsoft's Neo-Nazi Sexbot Was a Great Lesson for Makers of AI Assistants'. *MIT Technology Review,* 27 March 2018. Online: www.technologyreview.com/s/610634/microsofts-neo-nazi-sexbot-was-a-great-lesson-for-makers-of-ai-assistants/

Négyesi, Imre, 'A mesterséges intelligencia katonai felhasználásának társadalmi kérdései'. *Honvédségi Szemle* 149, no 1 (2021), 133–144. Online: https://doi.org/10.35926/HSZ.2021.1.10

Porter, Jon, 'Another convincing deepfake app goes viral prompting immediate privacy backlash'. *The Verge,* 02 September 2019. Online: www.theverge.com/2019/9/2/20844338/zao-deepfake-app-movie-tv-show-face-replace-privacy-policy-concerns

United Nations, *Final report of the Panel of Experts on Libya established pursuant to Security Council Resolution 1973 (2011), Pub. L. No. S/2021/229.* Online: https://digitallibrary.un.org/record/3905159?ln=en

Varga, Gergely, 'A vesztfáliai szuverenitás érvényessége a nemzetközi kapcsolatokban'. *Nemzet és Biztonság* 8, no 1 (2015), 30–38.

Vergun, David, 'Artificial Intelligence Key to Maintaining Military, Economic Advantages, Leaders Say'. *U.S. Department of Defense News,* 09 April 2021. Online: www.defense.gov/Explore/News/Article/Article/2567486/artificial-intelligence-key-to-maintaining-military-economic-advantages-leaders/

Vogel, Sandra, 'More Digital Assistants than People by 2021 Says Ovum'. *Internet of Business,* 15 July 2021. Online: https://internetofbusiness.com/digital-assistants-2021-ovum/