





Autonomous Systems and Cyberspace: Opportunities for the Armed Forces

Jakub Fučík¹ , Libor Frank² , and Richard Stojar² 

¹ Cyber and Information Warfare Command, Czech Armed Forces, Kounicova 65, 602 00 Brno, Czech Republic

jakub.fucik@unob.cz

² Centre for Security and Military Strategic Studies, University of Defence, Tučkova 23, 602 00 Brno, Czech Republic

{libor.frank,richard.stojar}@unob.cz

Abstract. The development of autonomous systems represents an opportunity for states to enhance their military power and change their status in the system of international relations, probably with the presumptions of the new Revolution in Military Affairs (RMA). Characteristics like flexible deployment, efficiency, adaptability, rapid upgradability, and/or the capacity to absorb losses that crewed systems cannot constitute potential game-changing technology in terms of military capabilities. The usage of the autonomous systems may vary from support functions (such as intelligence gathering, reconnaissance, or transportation) to coercive ones (autonomous weapon systems) in different operational domains. However, all types share a common characteristic – their interconnection with information technologies and cyberspace. Features like the complex structure, absence of specific borders, and diminished role of distance clearly distinguish this domain from land, sea, air, and even space and change the logic of how the security is provided there. Autonomous cyber systems (ACS) that operate in and through this domain represent unique military systems even among autonomous systems themselves. This paper aims to examine the interconnection between ACS and cyberspace and identify opportunities for a state's military power represented by armed forces. This relation addresses not only the dependency of the ACS on cyberspace and cybersecurity but also possibilities to enhance the cyber capabilities of the state to promote its national interests. The paper will focus on opportunities of the relation between ACS and cyberspace for capabilities of the NATO member states' armed forces. The Main Capability Areas (MCA) analytical framework will be used to analyze these aspects. Orientation on Prepare; Project; Engage; Sustain; Consult, Command and Control; Protect; Inform areas will identify opportunities to develop the full spectrum of potential capabilities and highlight main aspects of the transformation of the armed forces.

Keywords: Autonomous systems · Armed forces · Cyberspace · Main capability areas

1 Introduction

Nowadays, the armed forces of more than eighty countries worldwide are using remotely controlled Unmanned Systems (UxS) for reconnaissance, survey, or monitoring purposes [1]. The number of states which employ armed UxS is also gradually growing. We can assume that this general trend, i.e., the growing number of states which operate UxS of various categories, will only intensify in all physical military domains (land, sea, air, space). Compared to remotely controlled systems, the Autonomous Systems (AxS) require no or only minimal human operator involvement [2]. Individual systems should be able not only to obtain information about the environment but also to process (evaluate) this information and take appropriate decisions on their own. The motivation to establish those systems is directly based on their increased effectiveness in combat. Similar to remotely controlled systems, the idea of minimizing the human losses on the part of the operator's armed forces plays a key role [3]. Moreover, AxS enable to reduce (or altogether remove) the cognitive load of their operators. The development of AxS represents an opportunity for states to enhance their military power and change their status in the system of international relations. All mentioned features fundamentally distinguish AxS from "traditional" conventional weapon systems. They create new ways of warfare and even make the current one obsolete. This status establishes the new Revolution in Military Affairs (RMA) presumptions. All types of AxS share a common characteristic – their interconnection with information technologies and cyberspace. Features like the complex structure, specific borders, and diminished role of distance clearly distinguish this domain from land, sea, air, and even space and change the logic of how the security is provided there.

Autonomous cyber systems (ACS), which operate in and through this domain, represent unique military systems even among autonomous systems themselves from this point of view. This paper aims to examine the interconnection between ACS and cyberspace and identify opportunities for the state and its military power represented by armed forces. This relation addresses not only the dependency of the ACS on cyberspace and cybersecurity but also possibilities to enhance the cyber capabilities of the state to promote its national interests. The paper will focus on opportunities of the relation between ACS and cyberspace for capabilities of the NATO member states' armed forces. The findings within this paper were verified through expert meetings and workshops with the participation of members of the Ministry of Defence of the Czech Republic, the Czech Armed Forces, and representatives of the security community of the Czech Republic. Data gathering and evaluation on these events were carried out through the combination of structured interviews, questionnaires, and nominal group technique methods. Analyses of the opportunities are in this paper divided into several chapters. Section 2 discusses trends in the development of cyberspace which is mainly related to the transformation of the security and operational environment as well as to elements of military power. This chapter also provides necessary information for evaluating opportunities (see below). Section 3 provides general characteristics of the AxS and pinpoints on specificities of the ACS. Section 4 defines the theoretical framework of the paper – Revolution in Military Affairs and Main Capability Areas – which serves to identify and evaluate the opportunities for armed forces. Finally, Sect. 5 discusses opportunities arising from the connection between ACS and cyberspace in the set-theoretical framework. Through this

analysis, the paper should contribute to the discussion about the possible enhancement of NATO member states' military capabilities through ACS.

2 Cyberspace

Strengthening the strategic importance of cyberspace is directly linked to the development of information technologies and their use in virtually all areas of human life. Information globalization enables any actor (state and non-state) to have almost instantaneous and unrestricted access to a vast amount of data and their subsequent processing and use for their own needs. In this sense, the information became a strategic commodity usable both for shaping the position in this dimension and the functioning of the real environment. From the perspective of state and non-state actors, ensuring permanent and secure access to this domain is a prerequisite for the effective fulfillment of their interests. In this sense, the so-called cyber-attacks or malicious cyber activities - for example, in the form of the ability to deny an opponent's access to this domain and degrade his ability to exploit his systems or deliver harmful effects to our - represent essential tools for achieving the set goals [4], which are generally characterized not only by a very favorable utility ratio (investment/profits from the discussed activities) but also reduced ability to attribute such attacks and low probability of retaliation from the harmed entity.

The development of the Internet of Things (IoT) is gradually evolving into the Internet of Everything (IoE), which not only facilitates more effective use of the comprehensive information links (e.g., to ensure monitoring and decision-making in real-time) but also deepens the overall dependency on the stable and efficient operation of this space, resulting in user vulnerability. Building and developing 5G information networks take the discussed issue to a qualitatively higher level, both in terms of opportunities (faster data processing and bandwidth expansion) and potential threats (more vectors through which adversaries can attack). Ensuring security to particularly critical information infrastructure must consider this trend. This presumption is especially valid if we look at the potential abuse of devices within the so-called botnets to conduct targeted attacks against the information systems of both relevant state and non-state actors (for example, attacks on the availability of Telegram services in Asia in 2019 [5]).

Simultaneously intensifying the interconnection of humanity within this area increases the number of networks created and used on the distributive principle, i.e., without the existence of a central control or management "node". One such approach is the so-called "blockchain" technology, which is used by current cryptocurrencies and is gradually being introduced in other areas (e.g., banking or data and supply chain management and sharing) [6, 7]. The final form of this trend is an increase in the importance of the so-called "deep web", or in a narrower sense with the security connotations of "dark web" and "darknet" [8].

Notably, the dark web/darknet is directly linked to illegal activities across all areas (from illegal information gathering to trafficking in arms, addictive substances, or people). In addition to organized crime, similar means/possibilities are used, for example, by terrorist organizations and, in principle, by the states themselves. The consequence of this development is a further weakening of state power in the ability to control and regulate the activities and actors concerned and intervene against them as needed. This

situation causes conflict between the protection of national interests on the one hand and the utility of such networks on the other hand. The interdependence of all areas of human society with cyberspace further develops a dependence on the availability of information. The digitalization of state administration and the transfer of links between the citizen and the state into this domain (e.g., in the form of electronic identity cards or elections) directly reflects this phenomenon, which, however, also brings new forms of vulnerability (e.g., the issue of manipulation with electoral systems). From this perspective, the Internet allows increased transparency in almost all activities in the real environment. Social media, such as Facebook, Instagram, Twitter, YouTube, or TikTok, allow almost constant monitoring and keeping track of the activities of individuals. At the same time, it serves as an ideal tool and platform for conducting information operations by both state and non-state actors. Therefore, the capacity to monitor these networks or their providers can be considered as an essential prerequisite for controlling and influencing public opinion in general. On the other hand, this aspect helps defend against a potential adversary's meaningful activities effectively. Building the independent Russian "Internet" RuNet (successfully tested in 2019 [9]), or increasing the effectiveness of the so-called "Great Chinese Firewall" [10] in this respect, combines the two characteristics discussed above.

Fundamental importance (not only) for this domain will be the full implementation of quantum (computational) technologies, which by their very nature surpass the performance of individual computing systems. Consequently, new possibilities such as processing and storing extensive data (Big Data), calculating corresponding threats/opportunities for current encryption tools and procedures, i.e., protecting data and information itself, are associated with this. In January 2019, the first "commercial quantum" computer (IBM Q System One) was introduced [11]. Quantum technologies have the potential to enhance the capabilities of AxS and their performance. Significantly ACS could benefit from mentioned big data processing and the possibility of preparing and running more complex scenarios and prediction models or algorithms [12]. On the other hand, these are still the first explanatory steps, and ensuring the widespread use of this technology is still a matter of long-term research and development.

3 Autonomous Systems

The development of AxS is mainly related to the development of information technology, where many factors enable the creation of systems capable of performing enormous amounts of calculations per second. Along with the advancement of robotics and mechatronics, it is now possible to create robotic systems with capabilities that fell into the science fiction category a decade ago. Individual systems should be able not only to obtain information about the environment but also to process (evaluate) this information and take appropriate decisions on their own [13]. By general definition, autonomy is the ability of an entity to make conscious, unforced decisions. To describe nuances among AxS, it is necessary to express the level of autonomy concerning the environment and the role of the human operator. For military purposes, there are several definitions of the level of control or the level of independence of the system on the

human operator. Scharre, for example, distinguishes among semi-autonomous (Man-In-The-Loop), autonomous with supervisor (Man-On-The-Loop), and fully autonomous without supervisor (Man-Out-Of-The-Loop) systems [14].

The motivation to field these systems as soon as possible directly results from the increased demand for higher combat efficiency. As in the case of remote-controlled devices, the idea of minimizing casualties of own or friendly armed forces and non-combatants is represented [15]. Systems based on AI/machine learning elements more effectively suppress and eliminate human beings' physical and psychological limitations (including the need for sleep and the effects of fatigue or stress).

On the other hand, there are unanswered severe ethical and legal questions, e.g., the degree of autonomy that should these systems enjoy, and whether, at least from an ethical point of view, a decision to use force against human being can be taken purely by AxS [16]. This aspect is increasingly being discussed throughout the professional community [17] and is becoming a motivation for efforts to establish and enforce the arms control regime at the international level (e.g., under the auspices of the UN) [18]. On the other hand, it is necessary to point out that, following historical examples (e.g., cluster munitions or anti-personnel mines), the probability of achieving an overall ban across all states and enforcing it is somewhat unrealistic.

We can identify some aspects of these technologies on Guardium vehicles that can operate in a semi-autonomous mode [19]. Similarly, these elements are used in long-range missions of unmanned drones, where the human operator takes control of the UAV in the target area or surpasses air defense systems (e.g., the Phalanx point defense system) [20].

Furthermore, we can identify the considerable potential of the ACS based on AI/machine learning elements. The virtual identity of these systems ensures that they are most suitable to adapt to the regularities of cyberspace and fulfill tasks like the collection, evaluation, and processing of data and information in general. Their development and performance bring new possibilities, for example, for the detailed analysis of a large number of documents, visuals, or audio records. Consequently, related to this is the ability to imitate such data accurately, make copies, or even give them brand new features (such as a virtual person) almost indistinguishable from reality/originals (so-called deepfakes). Inherent connection of the ACS and cyberspace also enable further exploitation of this domain and related trends (see Sect. 2).

4 Theoretical Framework

4.1 Revolution in Military Affairs

For the purpose of this paper, we define RMA as the process and condition of revolutionary changes in the nature or method of warfare based on the external manifestations (actions) which employ the threat of force or the use of force to achieve political aims [21]. The "revolutionary" then refers to the radical nature of these changes, which, concerning the original system and its elements, must occur abruptly *de facto* preserving just a minimum similarity (e.g., in features by which the system is identified). Therefore, we cannot speak of a progressive (gradual) transition and the establishment of new

elements into the existing framework and its evolutionary transition. Regarding the military dimension of this revolution, we can use the modified characteristics defined by Jeffrey R. Cooper, who speaks about: "... discontinuous increase in military capability and effectiveness" [22].

Relevant changes in the method of warfare are founded on a technological level with the introduction and use of advanced weapons and information systems (e.g., precision-guided munitions - PGM, unmanned aircraft, and remote sensing devices/sensors). From this point of view, the character of AxS (see Sect. 3) represent technology which disruptiveness is based on new opportunities (as well as threats) how-to, for example, deliver harmful effect and thus the transformation of ways of war [23].

The character of ACS further correlates with changes in the doctrinal dimension. They are represented by the establishment of the concepts of so-called System of Systems (SoS) and Network Centric Warfare (NCW). The first concept is based on two fundamental elements - information and integration (cooperation). The prerequisite amalgamates particular systems and components, such as command, control, computers, communications, and information (C4I), into one coherent functional framework [24]. This structure should provide situational awareness on the battlefield in real-time for all relevant components of the armed forces.

The second concept is associated with the very existence and use of communication links among the units on the battlefield and their integration into the mentioned framework. Their interdependence allows them to maximize utilization of their combat skills and, on the other hand, compensate for weaknesses (e.g., through almost excellent fire support, information about the enemy's intentions). Full use of this potential is connected, e.g., to the implementation of the so-called "swarming" tactic, which in itself implies synchronized and highly flexible combat deployment of a large number of small clusters (military units) [25].

In practical terms, the army, which fully applies both concepts, is allowed to interfere (invade) the opponent accurately at his most vulnerable areas to prevent his possible attempts to initiate counterattacks or enact countermeasures and therefore wholly take over the combat initiative and paralyze the opponent.

4.2 Main Capability Areas (MCA)

The character of the armed forces could be analyzed in many ways and approaches. To ensure that conclusions of this paper would be valid in terms of NATO's documents and planning processes (especially NATO Defence Planning Process), NATO's analytical framework will be used. This framework covers the spectrum of tasks and phases in military operations that armed forces should fulfill successfully and prepare their capabilities for them. The concept of Main Capability Areas covers all this necessary development. These capability areas demonstrate a complex approach to tools of the military power of (NATO) states with the ambition to identify the ideal composition of forces that would maximize the potential of each state and diminish the threats and risks. The analytical framework identifies seven areas – *Prepare; Project; Engage; Consult, Command and Control (C3); Sustain; Protect; Inform* [26]. Interconnection between cyberspace and ACS in terms of RMA will be in this paper analyzed in all these areas to identify possible opportunities.

Prepare subsumes capabilities to establish, prepare and sustain adequate presence at the right time, including the ability to build up forces, through appropriate and graduated readiness, to meet any requirements, keeping sufficient flexibility to adapt to possible changes in the strategic environment. *Project* represents capabilities to conduct strategic deployment of the armed forces in support of any NATO and national mission. *Engage* is characterized by performing the tasks that contribute directly to achieving mission goals within the context of collective defense, crisis management, and cooperative security. It includes all capabilities required to defeat adversaries as well as accomplish the goals of other non-combat missions. *C3* are capabilities of commanders to exercise authority over the full spectrum of assigned and attached forces in the accomplishment of the mission. Including, for example, the capability to communicate and coordinate with other actors who are present or involved in the operational area and effective information exchange with the political and military leadership. *Sustain*'s capabilities serve to plan and execute the timely support and sustainment of forces, including essential military infrastructure, transportation, military engineering support, contracting, supply/maintenance/services management, basing support, and health and medical support. *Protect* represents capabilities to minimize through a common multinational and holistic approach of Force Protection the vulnerability of personnel, facilities, materiel and activities to any threat and in all situations, to include towards the effects of WMD, while ensuring the Allies freedom of action and contributing to mission success. Finally, *Inform* subsumes capabilities to establish and maintain the situational awareness and level of knowledge required to allow commanders at all levels to make timely and informed decisions [27].

5 Opportunities for the Armed Forces

5.1 Prepare

Interconnection between cyberspace and ACS gains two fundamental features in *Prepare* capabilities. The first one subsumes the possibility to train and prepare all armed forces branches through ACS. The second one targets how to train/prepare AxS in other domains to enhance our armed forces. In the first case, ACS exploits trends such as virtual reality development discussed in Sect. 2. Cyberspace represents here a domain that enables the existence of such training programs and could be used as a training field for military personnel. Comply with the use of enhanced or virtual reality, ACS creates an opportunity to bring simulation as close as possible to the real world and scenarios. For example, soldiers would be able to employ even lethal munition against an (artificial) adversary without endangering another human person who would, in traditional scenarios, take this role. Simultaneously, ACS connection with cyberspace and related computing tools enables preparation, running, and evaluating much more complex and comprehensive (real-time) scenarios than human observers could implement. These features are even highlighted in the case of training scenarios in cyberspace. Even today, the insufficient technological development of power sources and other related scientific fields cannot limit the ACS in this domain. Practical application try to address, for example, Neural 3D holography project [28].

The second-mentioned feature – how to train physical AxS – cyberspace represents an ideal platform for effective and quality learning. Direct connection of the ACS to this

domain enables the development of required traits, skills, and knowledge faster and more effectively than would be possible through classical educational methods. Of course, nowadays, this process is mainly represented by machine or deep learning. However, we can presume that further development of cloud and edge computing. Related analytical tools could move this feature beyond this concept and, through new levels of complexity, evolve it into the possibilities of almost full-fledged AI. The critical challenge in this process is to ensure that these systems would learn what we want and need and diminish the possibility of “mislead and failed” cases.

5.2 Project

The almost non-existent influence of distance in cyberspace is further highlighted by the computing and processing power of the ACS. This feature enables the precise and simultaneous projection of much higher numbers of units and other armed forces components than is possible by traditional means and processes. Of course, outside cyberspace, “conventional” transportation components are valid and mainly establish projection capabilities. On the other hand, even in these domains, ACS could minimally enhance, for example, air or naval transports through synchronization and control of their components to, for example, reduce fuel consumption, or ensure efficient use of cargo space. In cyberspace, ACS can project power almost independently. Virtual domain diminishes any physical limitation, and AI can fully employ all advantages over human operators. The impact of establishing new capabilities or enhancing existing ones in this area is incredibly revolutionary if we discuss small military powers. The combination of ACS and cyberspace enables them to gain global military power projection, which would be almost impossible under different conditions.

5.3 Engage

Practically, even nowadays, elements of ACS could be deployed as full-fledged agents. All kinds of cyber operations are manageable by ACS. It does not matter if the task is to steal information about the adversary’s forces, disrupt his chain of command by DDoS attacks, or lead a disinformation campaign through its communication channels and even other (social) media. Contrary to human operators, ACS profit from their direct connection with cyberspace. They are part of it. Basically, and with a bit of imagination, we can consider cyberspace something like the natural environment for ACS. This feature ensures that these systems are best suited for operations in it. From this point of view, each discussed characteristic of the ACS provides enhancement and new possibilities for breaking through the adversary’s defense or fulfilling any other tasks. This presumption is highlighted by other mentioned tools such as quantum computing which would provide new levels of performance. For example, dedicated ACS could establish not only a botnet of “zombie” systems but a network of autonomous agents that will have the advantage of the hive mind [29]. Their operations will be much faster, precise, and less detectable than nowadays. The same advantages we can identify in information operations that influence or deceive the adversary. ACS has made the process of creating convincing fake videos much easier and faster [30]. So-called deepfakes impersonate ACS to perpetrate various information campaigns, including phishing attacks. Fake politicians or commanders

could deliver our messages with unprecedented credibility and reliability to the targeted audience. All these aspects enhance social engineering tools and potentially sow distrust into the capability to distinguish the real world from the virtual one.

5.4 C3

C3 capabilities and the role of ACS are deeply connected with the concept of Network Centric Warfare and System of Systems described above. Emphasis on complex interconnection among all elements of armed forces and network of functional links increases demand on communication systems and data gathering and analysis. This is another case where so-called Big Data is produced, processed, and converted into the information necessary for all elements of armed forces according to their needs. ACS could fulfill such tasks and provide a robust network even with (near) real-time functions. Simultaneously, ACS provides enhanced support to the decision-making process. At tactical, operational, or strategical levels, such support establishes ideal conditions for evaluation all possibilities, choosing the best one, and implementing it. In these terms, ACS also provides enhanced opportunities for modeling and simulations. Access to processed and evaluated Big Data creates a unique database for different M&S tools [31]. ACS ensures that this database will be up to date and employ mentioned tools in real-time, and constantly provide necessary information to command structure and even make well-timed and precise decisions in a given situation.

5.5 Sustain

The usability of ACS to enhance sustain capabilities can be identified through the whole logistic and support system. Some possibilities, such as reducing fuel consumption or efficient use of transportation capacities, were discussed earlier. However, ACS provides and ensures complex support to armed forces in this area. Through cyberspace and physical sensors, ACS could process data from all components in real-time. They can provide information about their status and needs, evaluate them and issue orders to relevant agents. For example, autonomous medical systems can monitor the health of the soldiers and, in the case of degradation, send proper help even the soldier realizes that something is wrong.

Similarly, an autonomous logistic system can provide timely supplies or repairs. Simultaneously, ACS is not limited to these tasks. They could prepare predictive models for future (logistical) conditions updated constantly through data processing and evaluation. Application in so-called Deep Logic Networks [32] effectively enables the allocation of available resources and diminishes the possibility of shortage or unavailability of services. Based on the level of autonomy, ACS could also set and maintain the whole structure of sustain capabilities and decide about employing them.

5.6 Protect

Protect capabilities in cyberspace are critical parts of credible and effective exploitation of the ACS and other information-based systems in general. In this case, cybersecurity

became the vital interest of all actors. The character of ACS is inseparably connected with information technologies and cyberspace itself. This nature implicitly creates vulnerabilities of the ACS, especially in terms of malicious cyber activities which could target these systems. It does not depend on if we discuss cyber sabotage or cyber espionage. Practically every system could be compromised and used against our interests. Also, the same threats are valid for every domain where AxS would be deployed. Essentially, adversaries could hijack an autonomous plane like an AI agent in cyberspace. This possibility should be considered at every level of decision-making (from tactical to strategic) and developing safety- and countermeasures reflecting the share of dependency on these systems.

On the other hand, ACS provides new possibilities to ensure credible security and defense (not only) in cyberspace. Contrary to human operators, AI can analyze, process, and even control vast data flows. Practically, this increases the probability of detecting any malicious cyber activity targeting our (information) systems and provides new tools to counter it. The same logic could be applied to possibilities of deepfakes identification and bolstering resilience against adversaries' information operations [33]. Simultaneously, ACS enhances capabilities to identify such attacks in the preparation phase and provide early warning and enough time to related authorities to react. However, such conditions are related to the interoperability of deployed systems. Without it, AI would not develop its full potential throughout the whole protected structure and its elements.

5.7 Inform

ACS' role in this area is deeply enrooted in possibilities from C3 capabilities. These elements manage to provide and control the whole network of sensors in every domain and follow-on communication among all components. Moreover, all intelligence disciplines (OSINT, IMINT, TECHINT, even HUMINT) are dependent on the capability to gather and analyze required information and provide it to stakeholders. Transmission and processing of all data in cyberspace help gain (near) real-time connection, which pace and throughput depend more on human limitations than on technical ones. ACS could also ensure that threat of the information overwhelming will be diminished. Permanent presence and information monitoring through these systems enable to filter off all data much more preciously and with a proactive approach to providing them to relevant subjects.

6 Conclusion

Autonomous systems and their interconnection with cyberspace represent opportunities and challenges for the NATO member states' armed forces. Opportunities can be identified in all Main Capability Areas - Prepare; Project; Engage; Sustain; Consult, Command and Control; Protect; Inform. Specific features of cyberspace combined with ACS characteristics like suppression and elimination of the human beings physical and psychological limitations (including the need for sleep and the effects of fatigue or stress) provide new possibilities related to information basis of every (military) operation and network of NATO member states' armed forces components. The development of ACS is also connected with enhanced exploitation of concepts System-of-Systems

and Network Centric Warfare in terms of Revolution in Military Affairs. In *Prepare*, opportunities arise not only in training and preparation of all branches of armed forces through ACS but also ACS themselves. *Project*, *C3*, *Sustain* and *Inform* areas could benefit from modeling and simulation capabilities and new ways of data processing. *Engage* area is influenced by the inherited relation between ACS and cyberspace. AI agents represent the most effective tool to fulfill set tasks in this domain. ACS could bolster the cybersecurity and defense of Allies' systems and counter malicious cyber activities in the *Protect* area.

On the other hand, the main challenges come from the discussed dependency of ACS on cyberspace and information technologies. This connection creates potential vulnerabilities that adversaries could exploit. Especially in *Protect* area is crucial to develop and implement safety- and countermeasures on every level of the military structure, which could at least mitigate them. There is also a need to ensure interoperability of deployed systems, not only with the allies within NATO but also internally, through generations of weapons and other hardware classes. Interoperability and mutual compatibility strengthen the resilience of the entire structure (robustness and substitutability) and increase the efficiency of individual elements.

References

1. Gettinger, D.: Drone Databook Update: March 2020. Center for the Study of the Drone at Bard College (2020). <https://dronecenter.bard.edu/projects/drone-proliferation/drone-databook-update-march-2020/>
2. Hodicky, J., Prochazka, D.: Challenges in the implementation of autonomous systems into the battlefield. In: 6th International Conference on Military Technologies, ICMT 2017, Brno, pp. 743–744 (2017)
3. Stojar, R., Frank, L.: Changes in armed forces and their significance for the regular armed forces. In: The 18th International Conference. The Knowledge-Based Organization: Conference Proceedings 1 - Management and Military Sciences, vol. 1, pp. 142–145 (2012)
4. NATO: Strategic Foresight Analysis Report (2017)
5. Shieber, J.: Telegram faces DDoS attack in China...again (2019). <https://tcrn.ch/2ZJgfbC>
6. Karl, A.: Blockchain Technology for Cloud Storage: This Looks Like Future. Tech Genix (2018). <https://1url.cz/yM4zC>
7. Kelly, J.: Top Banks and R3 Build Blockchain-Based Payments System. Reuters (2017). <https://1url.cz/vM4zs>
8. Sui, D., Caverlee, J., Rudesill, D.: The Deep Web and Darknet: A Look Inside the Internet's Massive Black Box. Wilson Center (2015). https://www.wilsoncenter.org/sites/default/files/media/documents/publication/deep_web_report_october_2015.pdf
9. Wakefield, J.: Russia 'successfully tests' its unplugged internet. BBC (2019). <https://bbc.in/2X7vyst>
10. Wyciślik-Wilson, M.: It is getting harder than ever for VPNs to break through the Great Firewall of China. Beta News (2019). <https://bit.ly/3gr4v32>
11. Russell, J.: IBM Quantum Update: Q System One Launch, New Collaborators, and QC Center Plans. HPC wire (2019). <https://1url.cz/kM4K2>
12. Swayne, M.: Four Ways Quantum Computing Will Change Artificial Intelligence Forever. The Quantum Daily (2020). <https://thequantumdaily.com/2020/01/23/four-ways-quantum-computing-will-change-artificial-intelligence-forever/>

13. Hodicky, J.: Modelling and simulation in the autonomous systems' domain – current status and way ahead. In: Hodicky, J. (ed.) MESAS 2015. LNCS, vol. 9055, pp. 17–23. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-22383-4_2
14. Scharre, P.: Autonomy, “Killer Robots,” and human control in the use of force – Part I. *Just Security* 7(1) (2014). <https://www.justsecurity.org/12708/autonomy-killer-robots-human-control-force-part/>
15. Stojar, R.: Bezpilotní prostředky a problematika jejich nasazení v soudobých konfliktech (The Unmanned Aerial Vehicles and Issues Connected with Their Use in Contemporary Conflicts). *Obrana a strategie* 16(2), 5–18 (2016)
16. Fučík, J., Frank, L., Stojar, R.: Legality and legitimacy of the autonomous weapon systems. In: Mazal, J., Fagiolini, A., Vasik, P. (eds.) MESAS 2019. LNCS, vol. 11995, pp. 409–416. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-43890-6_33
17. Autonomous Weapons: An Open Letter from AI & Robotics Researchers (2017). <https://goo.gl/X2N6CA>
18. Gill, A.S.: The role of the united nations in addressing emerging technologies in the area of lethal autonomous weapons systems. *UN Chronicle* 50(3&4), 15–17 (2018). <https://1url.cz/3zZjq>
19. Army-Technology.Com: AvantGuard Unmanned Ground Combat Vehicle, Israel (2016). <https://goo.gl/knZqWb>
20. Raytheon: Phalanx Close-in Weapon System: Last Line of Defense for Air, Land and Sea (n.d.). <https://goo.gl/Ky3RD1>
21. Gray, C.S.: *Strategy for Chaos - Revolution in Military Affairs and the Evidence of History*. Frank Cass, London (2005)
22. Cooper, J.R.: Another View of the Revolution in Military Affairs. Strategic Studies Institute (1994). <https://ssi.armywarcollege.edu/another-view-of-the-revolution-in-military-affairs/>
23. Worcester, M.: *Autonomous Warfare – A Revolution in Military Affairs*. ISPSW, Berlin (2015). https://www.files.ethz.ch/isn/190160/340_Worcester.pdf
24. Owens, W.A., Offley, E.: *Lifting the Fog of War*. Farrar Straus Giroux, New York (2000)
25. Alberts, D.S., Gartska, J.J., Stein, F.P.: *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP, Washington D.C. (1999)
26. NATO: MC 400/3, MC Guidance for Military Implementation of Alliance Strategy (2012)
27. NATO: C3 Taxonomy Baseline 3.1 (2019)
28. Choi, S., et al.: Neural 3D holography: learning accurate wave propagation models for 3D holographic virtual and augmented reality displays. *ACM Trans. Graph.* 40(6) (2021). <https://www.computationalimaging.org/wp-content/uploads/2021/08/NeuralHolography3D.pdf>
29. Ciancaglini, V., et al.: Malicious Uses and Abuses of Artificial Intelligence, p. 35 (2020). https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-of-artificial-intelligence.pdf
30. Lyu, S.: Deepfakes and the New AI-Generated Fake Media Creation-Detection Arms Race. *Scientific American* (2020). <https://www.scientificamerican.com/article/detecting-deepfakes1/>
31. Hodicky, J., Prochazka, D.: Modelling and simulation paradigms to support autonomous system operationalization. In: Mazal, J., Fagiolini, A., Vasik, P. (eds.) MESAS 2019. LNCS, vol. 11995, pp. 361–371. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-43890-6_29
32. Pandey, S.: Opportunities to use artificial intelligence in Army logistics (2019). https://www.army.mil/article/216389/opportunities_to_use_artificial_intelligence_in_army_logistics
33. Divišová, V., et al.: “The whole is greater than the sum of the parts” towards developing a multidimensional concept of armed forces' resilience towards hybrid interference. *Obrana Strat.* 21(1), 8–15 (2021). <https://doi.org/10.3849/1802-7199.21.2021.02.003-020>