"AUTONOMISATION"[1] OF SECURITY AND DEFENCE SYSTEMS

Col. Artur KUPTEL, PhD
a.kuptel@ron.mil.pl
Inspectorate for Implementation of Innovative Defence Technologies

Abstract

Development of systems with an evolving level of autonomy is among the most controversial and yet promising aspects of military forces' modernisation. The application of quasi-artificial intelligence in combat machines opens a new uncharted area of possibilities. In essence, these modifications aim to reduce the extent of human interference in the functioning of unmanned systems virtually to none. The potential risks are explored in dangerous scenarios, which consider that apart from offering far-reaching advantages of using platforms with autonomic capabilities, they can be used against humanity. These scenarios assume a pivotal role in forecasting possible directions for development of the armed forces. This paper attempts to determine the essence of combat systems autonomy while focusing on a few of the most sensitive issues. For a transparent and credible debate on combat systems autonomy, it is adviseable that no ambiguity is present in terminological, ethical, legal and technological complexities, whose misinterpretation may become a source of unnecessary understatements or even lead to distortion of the debate.

Keywords: autonomy, autonomisation, unmanned autonomous systems, levels of autonomy

1 It is author's intention to propose use this term as the basis of this article. The specific meaning of „autonomisation" has been explained in *Terminology* paragraph.

Introduction

Systems with evolving levels of autonomy, and in particular weapon systems and military capability, are one of the most complex and controversial issues in the present public debate. Nearly every emerging potential problem of autonomy, even unrelated to armed unmanned platforms, attracts immediate public attention.

Experts are constantly making an effort to solve problems related to limiting human interference in the functioning of machines. These issues, in fact, not only attract the attention of individual states but also of numerous international organisations which engage in deliberate discussions in an attempt to formulate realistic, evidence-based conclusions and recommendations. One such organisation, ICRAC, assumes the goal of these multinational endeavours is to build the awareness and knowledge on autonomous systems, to encourage interoperability and to provide substantive support in the development and operation of these systems, including defence against them should they be used by an enemy[2].

These international debates are focused on preserving openness and transparency in the development of the autonomous systems technology, with the intent of dispelling fear amongst concerned society and ensuring proper regulations in the field. While the general perspective presented in these discussions predominantly expresses the views of specific expert groups, this by no means exhausts the subject. Therefore, NATO and EU member states, including Poland, should actively and continually participate in this momentous debate.

One of the underlying objectives of this paper's analysis is to provide an answer to questions about the assumptions of limiting human interference (autonomy) in the functioning of security and defence systems. Moreover, in order to provide a comprehensive discussion on the subject, the idea of autonomy is discussed in detail along with other related concepts, such as determining levels of autonomy and their criteria for weapon systems, relevant legal and ethical issues, and, finally, the dilemma concerned with applying the present and emerging technology in

2 An example is the (International Committee for Robot Arms Control – ICRAC n.d.), which took the initiative to stop the uncontrolled development of ideas related to the autonomy and implementation of robotic arms in the armed forces.

question and its implications. The article touches sensitive issues related to the challenges to be met by armed forces in the near future; these are associated with rapid development and an increasingly widespread use of autonomous platforms on the battlefield. The gravity of the presented considerations is further heightened by the fact that in the longer perspective of time, these changes may prove revolutionary[3].

Terminology

The need for the core nomenclature unification results not only from the discrepancies in the understanding of key definitions in the international environment but is also dictated by the increasing interest of the Polish Armed Forces in obtaining unmanned autonomous platforms. This is important from the perspective of their correct implementation in the future. Therefore, prior to further analytical work, proper terminology and the differences between the following widely used terms will be clarified: *"platform," "system," "robot," "unmanned," "remotely controlled," "automatic," "autonomous," "autonomic," and autonomy."*

Unmanned systems and related terms have been widely investigated in the scientific literature (Bielawski, Perz and Rzadkowski 2018), which is why this article is primarily focused on systems exhibiting autonomous characteristics. In practice, finding significant differences between these concepts is quite challenging; therefore, focusing on the subject of autonomy, one must not concentrate on this connotation. Regardless of whether the problem concerns a platform, a system or a robot, it may be assumed, with a certain simplification, that in each case it will be a machine built of three key elements: sensors monitoring the environment, a CPU governing reactions to changes in the environment and instruments that enable interaction with the environment. This mechanical device may be *remotely operated* by a human operator, *act automatically* or *autonomously*, executing

3 The progress of works on unmanned autonomous platforms is evidenced by the fact that, *e.g.* some analysts predict the complete elimination of the human factor in marine anti-mine activities after 2020 (Davis 2006).

a previously implemented programme, or following a set of general rules translated into a machine action by means of artificial intelligence.

The term *remote-controlled* refers to the functioning of a system or an activity performed by a human operator and describes the controlling of a device from a physically remote location – *e.g.* by means of radio, ultrasonic, or infrared signals or by signals transmitted by wire, such as optical fibres. Therefore, with respect to an unmanned system (platform), remote control is broadly understood as an activity in which a human operator analyses video images or data from other sensors to directly control the system *via* a control device, while remaining physically separated from the controlled platform. The unmanned system is incapable of operating on its own: it requires continuous or nearly continuous control from an operator[4].

In terms of *automatic*, a Polish dictionary gives the following definition variations:

- performing activities independently, without human control;
- continuous fire, until the bullets run out, according to principles of gunnery;
- unconscious action, without conscious thought;
- spontaneous activity, automatic enthusiasm;
- enforcing a punishment without question, in accordance with the rules of criminal law (Słownik Języka Polskiego)

In the context of the system, however, the term is defined as a process that can be implemented from start to finish independently, with no need for human intervention. An automatic system should have fixed, unchangeable choice points, and be programmed to perform a fixed (finite) number of alternative actions, chosen in response to signals or stimuli received from individual sensors.

The term autonomic is often used interchangeably with the word *autonomous*, which might be misleading because of the difference in the basic meanings between these words. The word *autonomous* refers to such qualities as self-governance, sovereignty, independence (an autonomous republic); while *autonomic* to the

4 According to NATO's glossary of terms and definitions (*AAP-6 2014),* an unmanned aircraft that is controlled from a remote pilot station by a pilot who has been trained and certified to the same standards as a pilot of a manned aircraft.

characteristics of the nervous system (autonomic nervous system of internal organs acting independently of human will), as well as to the response to internal stimuli (stimulation). However, in the context of systems, *autonomic* relates to the study of self-regulating systems in the field of control, including the control of the electronic process, or to the systems' ability to manage (control) its own internal state and interaction with the operational environment.

Autonomy, similar to autonomous, is the subject of much controversy and is the source of ambiguous considerations. The term is derived from Greek and is a combination of the words *autos* – itself, and *nomos* – law. Therefore, in literary meaning, autonomy infers that an autonomous being is able to impose its own norms on itself and is self-determined. In relation to a man or a group of people, these theories are justified and clear beyond doubt, in the case of platforms and systems, however, the situation becomes slightly more complicated.

Autonomous devices should be capable of development and should follow a moral law that is independent of their creator's, or even opposed to it. Theoretically, a fully autonomous machine would be capable of exerting its own will. Such an understanding of autonomy, especially in the context of artificial intelligence, is different from the functional understanding, typically referred to in the debate on autonomous systems (Kopec 2016).

These dilemmas require that the concept of autonomy be precisely clarified. The lack of a clear and binding definition may potentially result in the emergence of an alternative path in the development of unmanned aerial vehicles with evolving autonomy. This, in turn, may lead to their use contrary to the intended purpose (*e.g.* by terrorist and criminal organisations).

Autonomy – the aptitude of a system, platform or software to perform tasks without human intervention, using behaviour based on the interaction between computer software and the external environment. The operation is conditioned by, *inter alia*, the need to accomplish the objective, the perception of reality, and the internal state or knowledge (Kuptel 2017). The performed autonomous actions are in response to causes and problems programmed to solve, the adaptation of a platform/an element of a system to a new situation, or are the outcome of self-learning. Certain autonomous functions may be limited depending on the performed task

(see level of autonomy). **The process of increasing the level of autonomy in the functioning of machines will be referred to as *autonomisation*.**

Unmanned autonomous platform – a platform without a crew (operator) on board, capable of executing tasks (movement, manoeuvre and operation) without external human intervention, *via* the use of specialist software.

Unmanned autonomous system – a system composed of an unmanned autonomous platform, necessary equipment and payloads, communication system, software and crew responsible for managing, programming and supervision.

The core definitions given in the preceding paragraphs are to offer insight into understanding why a given device is described as autonomous.

Levels of autonomy

With regard to autonomous systems, one typically speaks of a system in which only certain functions are performed autonomously. The present-day technologies are essentially automatic systems, programmed to execute only predefined and predictable operations. In practice, system function is typically man-operated, others are executed automatically, and only a small portion may be performed autonomously. The debate on the levels of autonomy in many cases serves as a means to divert attention from the crux of the matter, which predominantly concerns the sphere of politics, law and engineering – *i.e.* the *level of human control* over the machine, which is necessary and achievable.

While the autonomy of platforms or systems is an enticing prospect when it comes to attracting public attention, particularly for the purpose of promoting conferences or initiating research programmes, the term is somewhat erroneously used to describe an entire system, although constituting just a part of it. By way of illustration, it is as if we referred to planes as "radio platforms" owing to the fact that they are equipped with radio stations. **For this reason, what should be emphasised about autonomy is that it is a certain technological capability over which an appropriate level of control is essentially maintained.** Determining levels of autonomy is necessary for the efficient and correct transfer

of control between elements of the system, *e.g.* the ground control and the platform performing operational tasks. As mentioned in preceding paragraphs, platforms and unmanned systems perform tasks being either remotely-controlled by a human, automatically or autonomously following previously programmed instructions or a set of general rules translated into a machine using artificial intelligence techniques. This is the simplest division of autonomy.

In practice, such categorisation is insufficient. Classification determinants should embrace physical parameters, tactical and technical capabilities, operational environment or the method for the assigned task execution. These elements are addressed by the classification employed by the US Navy Office of Naval Research, which has proposed a six-level scale of security and defence system autonomy (Williams 2008).

Level I. Human operated – all system processes are operator's reactions to external factors. The system is incapable of autonomously managing the environment in which it operates (although it may possess information about it), it only responds to recorded data.

Level II. Human assisted – the system performs activities in parallel with its operator, in response to external data; the purpose is to increase the ability of a human to execute an assigned task; however, the system does not act unassisted.

Level III. Human delegated – the system activity is limited by the delegated permission level and may include automatic flight control, or control over the engine and other subsystems, which are essentially human-activated and deactivated, and are mutually exclusive with human-controlled activities.

Level IV. Human supervised – the system can perform a variety of activities in a wide range of assigned permissions or instructions. Sufficient supervision and control over the system's internal operations and behaviour are provided (the functioning of a system is clear to the human operator and can be appropriately redirected). The system cannot self-initiate behaviour outside the scope of currently performed tasks.

Level V. Mixed initiative – both the human and the system can initiate action based on the acquired data. The system can coordinate its behaviour in an explicit

or implicit manner. The human understands the behaviour of the system in the same way as they understand their own. Diverse means are provided for regulating the system's authority with respect to the operator's presence in the system.

Level VI. Fully autonomous – the system does not require human interaction to perform programmed activities in a full range of different environmental conditions.

Fundamentally, the top level should never become available (in particular for the armed systems), and serves only as a reference point in the development of technologically advanced platforms. Although notably detailed and clear, this classification is still incomplete. Technological advances have out-paced this classification scale. Hence the ongoing works on the diversification of levels of autonomy with regard to the relevant functions of unmanned systems and platforms, *i.e.* core function, intrinsic function and support function (Kuptel 2017).

Changes in the art of war

From the technical perspective, platform *autonomy* is a set of complex algorithms determining and influencing the appropriate behaviour and effective execution of assigned tasks. These capabilities are enhanced through implementation of modern technological solutions that ensure optimal operation in various, rapidly changing conditions of the operational environment. The increasing requirement for autonomy in military capability is bound to have profound implications for security and may provide a critical edge when confronting contemporary hostilities. Platforms exhibiting different levels of autonomy are increasingly frequently encountered in everyday use. The most desirable solution for the widespread use of autonomy can be seen in the development of artificial intelligence. However, the fundamental counterargument is the potential misuse of such platforms resulting from the limited human control over the machine or lack of it.

Therefore, with respect to the autonomy of security and defence systems, it is relatively safe to presume that the classical assumptions of the art of war are on the verge of substantial revision. The character of warfare is changing – and has been for a number of years. Some argue that so too will the nature of

war. This revolution concerns not only the warfare itself but also its particular components, *i.e.* strategy, the operational level of war and tactics[5]. Results from the implementation of innovative technologies are bound to trigger fundamental changes in modernisation of defence systems leading to improvement in their capability. It is believed that unmanned autonomous systems exhibit the necessary potential to change not only the "rules of the game," but the "game" itself – moreover, such transition has already occurred in the history of warfare.

The evidence of such evolution can clearly be seen in the case of the tank. During the First World War, the tank was introduced into the battlefield primarily with the aim of improving the efficiency of crossing difficult terrain. However, subsequent modifications to its armaments and fitting additional means of communication have led to a breakthrough in the tactics and value to the operational level of war activities. With respect to autonomous systems, it is difficult to project the course of future development aspects as they affect the operational principles of war, the defence doctrine, planning, policy and procedures. However, the change that will most certainly occur concerns the fact that what has so far been reserved for the human domain (*e.g.* decision making, reasoning) can soon be integrated into unmanned autonomous systems. As a consequence, the very foundations of Clausewitz's theory of war[6] are likely to evolve in order to accommodate the problem of "defeating" autonomous systems. Thus it seems necessary to undertake common effort aimed at developing methods (technologies, tactics, techniques and procedures) that would enable not only the use of such systems but their protection against the effects of the use of autonomous systems by an adversary. The current state of knowledge, equipment and standing operating procedures do not accommodate the surge of autonomy as a critical component for capability and future operational advantage. This will soon change.

5 The art of war is the theory and practice of armed warfare. The sense of the term is twofold: firstly, it is a theory whose subject is preparation and execution of hostilities; secondly it concerns the operation mode of command and combat forces in the preparation and conduct of combat; (Koziej 1993, p. 25).

6 According to Clausewitz's classical theory, the pure concept of war encompasses destruction of the enemy's armed force, conquest of the enemy's territory and breaking the enemy's will to continue the struggle.

Ethical and legal aspects

The use of machines with autonomous operation capabilities, particularly those with a decision-making capability regarding selecting and engaging targets, requires resolving an array of dilemmas lying at the intersection of ethics and law. Therefore, considering these aspects becomes indispensable for proper evaluation of autonomous platform technologies *per se*, as well as determination of their future development direction. The issue has already been approached, for instance in the *Concept for the Use of Unmanned Autonomous Aircraft Systems [Koncepcja wykorzystania bezzałogowych systemów autonomicznych w Siłach Zbrojnych RP]*, which highlights the following potential ethical problems related to autonomous combat systems (*Koncepcja wykorzystania bezzałogowych systemów autonomicznych w Siłach Zbrojnych 2016)*:

- From the ethical perspective, holding constructors responsible for the behaviour of a fully autonomous platform is unjustified, as is blaming parents for the actions of their adult children.
- It will be immoral to use armaments, which by definition cannot be fully controlled.
- In Western culture, not only the reason for taking life but also the method is important.
- The ethical dimension is not limited to the extent of the cause-and-effect relationship, which occurs in machines.
- Depriving armed conflicts of ethical elements characteristic of a human being will lead to unacceptable events on the battlefield.
- Keeping man in the decision chain alone is by no means an effective solution for legal and ethical dilemmas.
- The premises of humanitarianism and the Martens clause[7] have been the basis for prohibiting certain types of weaponry (gas warfare agents, chemical weapons and laser weapons).
- Randomness of behaviour is not autonomy.

7 The clause included in the preamble to the 1907 Hague Convention (IV) with respect to the laws and customs of war on land; named after the Russian delegate Fiodor Martens, who had introduced it. It refers to accidents not covered by the provisions of the Fourth Hague Convention relating to war on land. According to the Martens Clause, in these situations, populations and belligerents remain under the protection and the principles of the international law, arising from the customs established between civilised nations and from the laws of humanity the requirements of the public conscience (Dziennik Ustaw of 1927 [Journal of Laws] No.21, item 161)

The list above does not exhaust all aspects of an ethical nature; however, these points should be considered in analysis prior to deciding whether to employ unmanned autonomous weapon systems. They may be regarded as the litmus test for the socially binding moral standards, and therefore deserve the status corresponding with the legal and technical considerations of employing such systems. Under no circumstances must future conceptual works regarding autonomous platforms exclude the ethical aspects of their functioning, as it could potentially lead to growing social resistance in this matter. Also at the design, construction and programming levels, it is fundamentally important that the developers of unmanned autonomous platforms follow certain norms, understood as the ethics.

From the legal perspective, the problem is more complex due to the existence of a number of relevant international norms and international judicial bodies, including International Humanitarian Law (IHL); Article 36 of 1977 Additional Protocol I to the Geneva Conventions of 1949, judicature of international judicial bodies, headed by the International Court of Justice (ICJ) in the Hague, and the European Court of Human Rights (ECHR) in Strasbourg, European Convention of Human Rights (ECHR), and the International Covenant on Civil and Political Rights (ICCPR) (Kuptel and Williams 2014).

According to experts, in its current legislative state, the international law does not prohibit the development of this technology nor does it prohibit its deployment in hostilities, furthermore, there is little likelihood that unmanned autonomous platforms could ever be deemed illegal. Therefore, the legal analysis will largely depend on the type of store carried by autonomous systems, and in particular the rules for their employment and potential engagement. Considerable doubt may be raised by the question of delegating autonomy with regard to *Core Functions* (Kuptel and Williams 2014)[8]. Therefore, there is a pressing need to further the research undertaken by individual member states with the objective of confirming the conclusions of the international team of the Multinational Capability Development Campaign. It is in the interest of all countries involved in the development and usage of autonomous technologies to provide reliable

8 The main functions for which the system was created and for which the eventual related payloads are installed, for example: firing, ISR, jamming, transport.

confirmation of the interpretation of current international laws and court judgments with regard to unmanned autonomous platforms.

A proliferation of studies into autonomisation of security and defence systems has coincided with the emergence of international organisations whose intent is to undermine the legitimacy of conducting further research in the field. This has been seen in the case of the previously mentioned organisation, ICRAC, whose efforts have led to a debate in the United Nations on limiting/prohibiting the use of autonomous security and defence systems, concluded in the *United Nations Convention on Certain Conventional Weapons (CCW),* Lethal Autonomous Weapon Systems (LAWS). As a result, in 2016, one of the largest Canadian companies from the advanced unmanned systems sector became the first to officially join the *Stop Killer Robots* campaign, guaranteeing that their technologies will not be sold for military purposes (International Committee for Robot Arms Control).

Command and Control

The concept of autonomy also refers to the interaction between the operator and the autonomous machine or, in a wider perspective, between the commander and human-machine teams. What is predominantly subject to change is the philosophy of unmanned autonomous systems control. In autonomous systems, the operator's task is to define objectives to attain, rather than to implement specific instructions (tasks) for achieving them. With regard to commanders, owing to the implementation of intelligent tools aiding the decision-making process, their management capabilities are enhanced, thus enabling them to control considerably larger teams composed of manned and autonomous systems. The developments in question fit in with the ongoing efforts to reduce the personnel burden; however, simultaneously there exist some doubt regarding the capability of autonomous systems for human-machine interaction with manned platforms. These issues are also considered in a broader perspective, in terms of the entire command-and-control system, in particular regarding synchronisation of activities and battlefield management (Kuptel and Williams 2014).

As the number of autonomously executed machine functions rises, the amount of data exchanged in the machine-machine, machine-human and human-machine teaming is expected to increase rapidly. In addition, the level of decentralisation in military structures is likely to increase as well, which can already be seen because of advances in the field of information and communication technologies (ICT). In the last two decades, these were centralised command and control centres that directly handled the movement of platforms. However, in the foreseeable future, highly-decentralised command and control centres, supported by highly flexible and efficient IT network management systems, will inevitably be deployed within and outside the theatre of operations to provide machine-machine communication with minimised human operator control/input.

The control networks can become integrated at all command levels while being provided with an up-to-date comprehensive common operational picture. This may lead to ambiguity in the boundaries of the operational and tactical levels of command. Autonomy in both areas, *i.e.* in systems control and decision-making support, allows commanders to control very large teams in extremely demanding and dynamically changing conditions. This will necessitate redefining the core assumptions of the defence doctrine and the manner of conducting military operations. As a core military function, the definition and practice of command and control may well need revision due the irreversible impact of this technology.

In light of autonomy, the discussed system of command and control should be considered in a wider perspective, particularly in terms of translating the original "intention of the superior" into defining the objectives of machines' activities so as to ensure their coordination at all levels of command. As the amounts of data collected, processed and controlled predominantly by machines are soaring, the need arises to define the methodology for determining the *accountability* of a system – in order to understand why an autonomous platform has done what it has done.

The increasingly widespread application of new technologies in the decision-making process and in command-and-control systems is likely to similarly affect the personnel, who will be required to adapt their skills to the arising requirements of the military of the future. For example, while a classically-trained pilot officer remotely-controlled a single unmanned aircraft, his role may evolve into that of

a system manager in the near future, who will be responsible for the control of entire swarms of autonomous systems (Grenda 2017).

There is a distinct probability that new areas of competence and skill in the field of security and defence system autonomy will emerge. New criteria of capabilities are bound to be distinguished to encompass the system management skills, and furthermore, greater importance will be ascribed to technical ICT skills and the development of tactical methods for the implementation of new technologies. The changes in question can have a dramatic impact on our military culture.

Among the fields that may potentially benefit the most from the emerging autonomy technology is training. Assuming that the behaviour of autonomous systems is determined by computer algorithms, the same algorithms may be modelled in simulation to provide a realistic training environment, thus reducing costs while not compromising the training requirements. It may be predicted that in the near future, the flight simulation technology could be more profoundly employed for training purposes, rather than in actual combat platforms (Grenda 2017).

Interoperability in multinational operations

One of the challenges associated with the use of unmanned autonomous platforms concerns the implications for their engagement in multinational operational activities. The broadening spectrum of military applications for autonomous systems is certain to fundamentally change the *modus operandi* of armies.

International operations involve a certain risk that their participants could differ in their approach to the involvement of autonomous technologies in action. One potential consequence of such discrepancies may be the distrust among allies due to the lack of common views, or discrepancies in skills or resources. Furthermore, some countries may be enthusiastic about using autonomous systems on the battlefield, while others strongly oppose (Grenda 2017).

With interoperability in mind, understood in terms of compliance with the rules for the employment of weapons as well as at the technical level, it is essential that international organisations work in consultation with their partners to produce

well-prepared staff, training and appropriate infrastructure. Regulating technical standards is of great importance. For example, in the Centre for Maritime Research and Experimentation (CMRE), several unmanned underwater platforms have been purchased from the same supplier at one-year intervals. During operation, it became apparent that platforms purchased in different years failed to communicate with each other, and the incompatibility was a result of substantial discrepancies in technological advancement between the generations of the product. One can only speculate on the potential scale of the problem on a regional or global level.

Bearing in mind the premise that autonomous systems are expected not to operate in a random or indefinite way, there is abundant room for further research and development work in the field of security and reliability standards for autonomous systems. Although there exists a general methodology in the field, which is a review of selected national practices related to the safe implementation of autonomous systems, it has been outside the scope of this study because of methodological limitations and the volume of this publication (Kuptel and Grutza 2017).

Summary

Implementation of autonomy in security and defence systems is a complicated and challenging process, which requires resolving numerous dilemmas. The considerations presented in this paper constitute only a partial synthesis of the body of knowledge, which is more systematically presented in the referenced literature. A note of caution is due here since the significant advantages of using autonomous platforms come with a certain risk. The implications of full autonomy go beyond the capability for executing tasks faster and at greater efficiency, reducing the risk of errors and the life threat; autonomy entails, on the other hand, the risk of losing control or risk of ruthless actions.

Another point on the list of crucial aspects of autonomy is the awareness that similar technologies are most likely being developed by countries whose intentions are far from unambiguous. To think that potential enemies are not making efforts to obtain such systems is delusional. While the advances in autonomous platforms imply a completely new type of threat, the barrier to overcome in order to gain access to these new technologies is relatively low. Admittedly, in contrast

to civilised and law-abiding states, adversaries are likely to use these systems in a manner that is contrary to international law, including deployment of kamikaze attacks, autonomous drone swarms systems and cyber hacking of such systems. However, it appears that the last-mentioned case seems to pose the most serious threat, as the compromised (hacked) systems can be used against friendly forces.

In order to make the most of the implementation of this new promising technology, it is vital that the military segment and the research and scientific communities cooperate in close coordination, due to the fact that there is a strong probability that a machine's capability for decision-making will generate considerable controversy. Furthermore, combined with military equipment, these dilemmas become even more complex. In the preceding sections, a few key areas were indicated in which multidimensional, national and international cooperation should be continued and include more advanced and comprehensive research works. The current stage of developments in autonomy is but the initial phase of a breakthrough era related to the autonomy of security and defence systems. Apart from tracking the developments in military technologies, an equal amount of attention should be given to the developments in civilian systems. For example, the USA has passed laws that permit road tests of autonomous cars. For many, this is a controversial idea; however, cars tested by Google, Uber and Tesla can offer unprecedented opportunities, such as the prospect of independent travel for the blind and the disabled, and potential future implementation in public transport or industry. Nevertheless, whenever considering such technologies, one needs to bear in mind the situations referred to in the introduction to this work.

Caution must be applied when employing (humanistic) concepts such as autonomy, intelligence or emotions to determine the characteristics of machines – such as autonomous robots or intelligent platforms – as it may be the source of much confusion and misinterpretation. Public opinion is spooned with potentially misleading views on autonomous systems, which triggers a vigorous media response aimed at producing dramatic news. In fact, fully autonomous robots wandering the battlefield unattended are and should remain in the realm of science fiction.

Further works under the *Convention on Certain Conventional Weapons* LAWS are due as they can lead to developing constructive solutions to numerous issues at the legal, ethical and social level regarding combat and non-combat

autonomous platforms. The danger is in the lack of precise legislation in terms of autonomous platforms, which might result in their deliberate use against the original purpose.

Launching works on the development of unmanned systems with an evolving level of autonomy may serve the purpose of identification of potential threats, as well as of establishing methods for avoiding, counteracting or at least weakening their effects. It is of vital importance to provide commanders and support personnel with necessary education so as to ease them into the acceptable coexistence and common understanding of the upcoming revolutionary technology. The lack of a certain degree of awareness, positive perception and confidence in autonomous platforms may prove crucial for their effective introduction and operation.

In order to ensure proper control over the development of this breakthrough technology, it seems reasonable to create a special interdisciplinary working group composed of representatives of the Polish Armed Forces, constructors, producers, lawyers and representatives of other sciences (ethics, psychology and social sciences), who would perform advisory functions in the progress and deployment of autonomous platforms. This group would constitute a consultative body for the appropriate state entities, personnel of armed forces and producers seeking expert opinion, or looking to dispel doubts. For greater social transparency, the working of the group should be in part shared with the public for multidisciplinary use.

For the reasons presented in this work, it seems reasonable to continue the advanced research work to determine the opportunities and threats associated with the implementation of autonomy in security and defence systems, so as to increase the level of readiness for future challenges. Close cooperation between the military and the autonomous system developers, both in Industry and elsewhere, should be maintained striving for the integration of these works under the aegis of international programmes.

References

AAP-6 Słownik Terminów i Definicji NATO, 2014.

Bielawski, R., Rzadkowski, W. and Perz, R., 2018. Unmanned Aerial Vehicles in the Protection of the Elements of a Country's Critical Infrastructure – Selected Directions of Development. *Security and Defence Quarterly* 22(5).

Davis T.D., 2006. *Design, implementation and testing of common data model supporting autonomous vehicle compatibility and interoperability*. Naval Postgraduate School. Monterey, USA.

Grenda B., 2017. Nowe technologie w dowodzeniu siłami powietrznymi. In R. Bielawski, B. Grenda, *Bezpieczeństwo lotnicze w aspekcie rozwoju technologicznego*, pp. 118-144. Wydawnictwo ASzWoj. Warsaw.

International Committee for Robot Arms Control, n.d. [online] Available from: https://www.icrac.net/ [Accessed 25 Oct 2018].

Koncepcja wykorzystania bezzałogowych systemów autonomicznych w Siłach Zbrojnych RP, 2016. CDiS SZ, Bydgoszcz.

Kopeć, R., 2016. Autonomia systemów bojowych. *Przeglad Geopolityczny*. Vol. 17, 133- 147.

Koziej S., 1993. *Teoria sztuki wojennej*. Warszawa.

Kuptel A., 2017. Counter Unmanned Autonomous Systems (CUAxS): Priorities. Policy. Future Capabilities. [online] Available from: https://ssrn.com/abstract=2963835 [Accessed 26 Oct 2018].

Kuptel A., Grutza M., 2017. *Review of National Practices of New Technology / System Review and Supplemental Analysis*. Norfolk.

Kuptel A., Williams A., 2014. Policy Guidance: Autonomy in Defence Systems. [online] Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2524515 [Accessed 25 Oct 2018].

Kuptel A., 2014. *Zastosowanie bezzałogowych systemów powietrznych w aspekcie militarnym*. Wydawnictwo AON. Warsaw.

Słownik Języka Polskiego, n.d. [online] Available from: https://sjp.pwn.pl/ [Accessed 26 Oct 2018].

Williams, R., 2008. Autonomous systems overview. BAE Systems. [online] Available from: http://www.aircraftbuilders.com/files/2716/File/BAE_%20Systems_Text_Version.pdf [Accessed 25 Oct 2018].