POTENTIAL TARGETS OF CYBER-ATTACKS: LEGAL REGULATION OF DRONES AND SELF-DRIVING CARS

Ádám Perger

PHD student, Faculty of Law, University of Debrecen, Hungary

Abstract. *After the attacks of September 11, 2001, terrorism has become part of our everyday life again, and it is only right that research has been conducted to explore the possible transposition of traditional terrorism into cyberspace. The first question is whether cyberterrorism itself can be defined. The first such definition is that of Keith Lourdeau, former head of the FBI's cyber defence division, who defined cyber terrorism as 'a crime committed using computers and telecommunications facilities to disrupt and/or disrupt services, causing confusion and uncertainty in the public. These actions are intended to influence the government or the population by force in order to achieve an organisation's individual political, social or ideological goals. Professor Dorothy Denning also used similar language, writing immediately after 11 September 2001: "cyberterrorism is a computer-based attack or threat designed to intimidate or coerce governments or societies into achieving the political, religious, or ideological goals of a particular terrorist organization. At the same time, the United States of America routinely uses unmanned combat aircraft (armed drones) against terrorists in the Middle East. The use of military drones, however, raises a number of questions of military law and human rights, which have yet to be answered. The aim of my research is, in part, to show how the use of military drones in the 21st century can be assessed from an international law perspective, what the implications of the continued use of these tools will be, and how vulnerable these tools are to cyberterrorists*

Keywords: *millitary, cyber, drone, terrorism, data, defense*

1. Introduction

Let's say a country with drone technology launches its armed drones on the territory of another sovereign state because terrorist groups are hiding there. The question arises: is the sovereignty of the country concerned violated? After the events of 2001, the UN Security Council issued Resolution 1368, which recognised the terrorist acts of 11 September 2001 by al-Qaeda as a threat to international peace and security and recognised the US right to self- defence, thus recognising the events in New York, Washington and Pennsylvania as an armed attack. An attack such as the one in 2001 could trigger an invocation of the right of self-defence anywhere in the world, and thus possibly the issuance of a Security Council resolution or an armed order. It is important to note, however, that the BT does not have a role only in the adoption of such resolutions, since Article 51 of the Charter also provides that the right of self-defence may be exercised only until the BT has taken the necessary steps to maintain international peace and security; and that a state exercising the right of self-defence is also obliged to bring to the attention of the BT any measures taken in the exercise of that right.

However, countries using drones have so far failed to fulfil this obligation under the Charter. Article 51 of the UN Charter states that "Nothing in the present Charter shall prejudice the natural right of individual or collective self-defence in the event of armed attack against any Member of the United Nations, so long as the Security Council, in the interest of the maintenance of international peace and security has not made the necessary arrangements. Members shall promptly bring to the attention of the Security Council the arrangements made by them in the exercise of this right of self-defence, and such arrangements shall in no way affect the powers and duties of the Security Council under the present Statute to take at any time such measures as it may deem necessary for the maintenance or restoration of international peace and security." [1] It follows that the right of self-defence may therefore be invoked in the event of an armed attack against a Member State. Before analysing the issue from the perspective of international law, it is first necessary to deal with the drone itself.

2. About drones in general

The United States Federal Aviation Administration Modernization Act of 2012 states that a drone is a structure consisting of an unmanned or unmanned aircraft and the components necessary for its safe and efficient operation. [2] Unmanned Aerial Systems ("UAS") are therefore complex structures made up of two components. The first is the flying surface itself, which allows three-dimensional movement, and the second comprises the instruments and devices that are mounted on the first element.

The mobile platform on which the drones are based is the part of the system that can fly remotely or autonomously. [3] In the former case, the device is controlled by a human from the ground. However, it is now possible to pre-program the flight path using a computer on board the UAS or other communication devices. As a result, the system can autonomously, will perform the flight without external intervention, with human intervention only needed in an emergency. However, fully autonomous operation remains to be seen, and as far as we know, science has not yet reached the stage where UAS are capable of making decisions and

planning autonomously, so human intervention is still a constant but not necessarily necessary feature of drone operations.[4]

The technologies that make up the second component of unmanned aircraft systems can be divided into two groups. The first group includes systems that provide the control and communication link necessary to coordinate the movement of UAS. The second is a variable component consisting of solutions adapted to the function of the drone. UAS can be equipped with various information gathering technologies, such as high-resolution cameras, thermal and wall-viewing or eavesdropping devices, infrared or UV sensors. [5]

Possible applications also include various data processing systems, such as facial recognition or other biometric technologies.71 Drones can also track designated targets with the help of radars, GPS and motion trackers. [6] And the size, flight range and time of the whole system is determined by the flying platform. Based on this, a distinction can be made between small UASs, which are defined as drones that weigh less than 25 kilograms and fly less than 122 metres. Large UAS are defined as systems that are heavier, have longer flight times and are more expensive, the best known examples being drones for combat purposes. What a UAS can be used for is determined by the technologies installed on the flying structure. Today, when the average person hears the term 'drone', the first thing that comes to mind is the reconnaissance and strike detection equipment used by the US military, but there are now more than 400 different applications for unmanned systems used for non-military purposes.[7]

One of the main criticisms of current drone operations in the area of jus ad bellum is whether the right to self-defence can be invoked against a terrorist organisation, i.e. a non-state actor. In my opinion, it can. The problem of imputability should be mentioned here. Another important conceptual element of self-defence is the question of imputability: an armed attack must be committed by a state. [8] Provided that the terrorist organisation in question is under the control of the state concerned, or that the state in question provides shelter and/or support to terrorists, the acts of the organisation in question may be attributable to the acts of the state. The legitimate question is what happens if a "cyber-terrorist" manages to take control of an armed drone - owned or used by the State - and uses it to communicate its ideological messages or, if necessary, to start an international conflict, since the victim State will not know that the drone was controlled by a terrorist at the time of the attack. The issue is further complicated by the growing spread of the Islamic religion in Europe, which includes much easier hiding places for terrorist groups. [9] Obviously, general prejudice has been significantly curbed throughout history by major statesmen such as Kamal Atatürk. [10] This has led to a situation where Turkey's legal system consists mainly of written laws. [11]Obviously, the concept of citizenship is of paramount importance here, as it is a concept of strategic importance that is also central to the definition of identity, participation in power, the delegation of power, human rights and the public interest. [12] The above example clearly shows that in the context of military operations carried out by remote-controlled or entirely unmanned machines, a number of legal (military law, human rights, privacy) and ethical concerns have recently arisen, which have yet to be fully resolved and the questions raised answered in a reassuring manner. There are some opinions that unmanned aerial vehicles (UAVs), also known as unmanned aerial vehicles (UAVs), are a "drones" are well on their way to becoming "killer Killer Applications", a new technology that is not only lethal, but that changes the rules of warfare completely. It is difficult to predict what this turnaround will look like. In the opinion of many experts, unmanned systems are in the same situation today as automobiles were at the beginning of the 20th century."[13] Critics argue that the operators of remote-controlled combat equipment are losing their sense of responsibility because of the great distance from the actual site of deployment,[14] the lack of concrete experience of the destruction caused by the weapons, the "video - gamification of war" (video - gamification of war)[15] makes the decision to use weapons easier for those making the decision. [16] The former opinion is not shared by the crew members of unmanned aerial vehicles, who express a sense of responsibility and are aware are of their decisions the real consequences of their decisions. [17] In addition, experts acknowledge that drone operators, although not in immediate physical danger, are subjected to similar or even greater psychological stress and strain in the course of their work than if they were actually in the field. While flying their drone over the attacked target, they are immediately confronted with the "result" and the sight of the destruction during the mandatory battle damage assessment. In contrast to soldiers who carry out the task with "conventional" weapons (guns, tanks, gravity bombs)[18], SPARROW points out that the combatants közötti distance reduction not automatically implies greater adherence to humanitarian principles. Citing the examples of Kosovo and Rwanda, he notes that "the cruellest atrocities of modern times have been committed in relatively small areas by men armed with rifles and machetes."[19] In addition to the aforementioned questions, from a military law point of view, there is a serious question mark over the status of personnel operating unmanned devices, i.e. to what extent they can be considered combatants, a legitimate military target, especially in view of the fact that are not physically present in the area of operation? According to the current understanding, drone operators are as legitimate targets as other members of the armed forces, as they are actively contribute a military operations and therefore their person and "place of work" can be legitimately targeted. The issue is further complicated by the fact that some countries employ civilian personnel, employees of specialised civilian companies, as drone operators, rather than military personnel. Consequently,

these individuals lose their protected status and become legitimate military targets. Periodically, we also encounter the criticism that the development of drones and other military robots is directly contrary to the requirement of jus ad bellum, because it encourages politicians to go to war. The main argument is that the operator(s) remain in a safe environment and the mission is carried out by a machine, politicians are also more inclined to opt for this kind of armed conflict. The use of remotely piloted or self-propelled military equipment lowers the barrier to entry into war, as machines reduce the loss of manpower and hence the political cost of going to war. It can be concluded that the use of remotely controlled military devices and robots can lead to an increase in the number of armed interventions, because decision- makers can order military operations in the knowledge that they will not have to expect any or only a low loss of human life. [20] Altmann also highlights the risk of conflict-exploitation inherent in drones when he points out that unmanned aircraft are more difficult to detect because of their relatively low altitude and speed, making them easy to use to fly into another country's airspace without permission and carry out precision operations there. Such an operation, if it were to be discovered, would be likely to incur the displeasure of the leadership of the country concerned. The situation would be further complicated if the country concerned were to shoot down the device in self-defence.

Other opinions have been expressed on the subject, according to which some countries (e.g. Pakistan) tolerate such operations only because the equipment is unmanned, so that flying it over their borders does not constitute a border crossing by foreign soldiers, which they would not otherwise allow. Recognising the benefits of using semi- or fully unmanned assets, the world's major military powers took steps years ago to speed up research and deploy an increasing number of autonomous assets. The best example of this is the United States of America, where in 2005 a committee of experts proposed the acceleration of the integration of UAVs currently in production or under development into military operations for all branches of the armed forces and the full exploitation of their capabilities. [21] The latest US plan, which runs until 2036, calls for the use of unmanned equipment and new technologies in the military and continue to develop. It also requires the Ministry of Defence to strive for the systemisation of tools with a greater degree of autonomy in order to reduce the need for human resources and dependence on full-time broadband communications, as well as to reduce the time spent on decision-making processes. However, the document points out that when increasing the autonomy of machines, it is also necessary to take into account the financial possibilities, the operational feasibility, the new technological advances, the various guidelines, public opinion and the disadvantages of autonomy. [22] In addition to the US's emphasis on robotic technology, it is worth noting that the British armed forces, despite their use of unmanned aircraft, are far from having such ambitious plans. According to the UK Ministry of Defence's 2011 Joint Forces Doctrine on the s ubject, the UK, although at the forefrontof technological developments in many areas, has limited experience of operating modern unmanned aircraft capable of performing a given task and little operational analysis is available.[23]

The document highlights that, in the absence of higher-level political guidance, all unmanned aircraft systems used by the British Armed Forces were procured or leased under the Urgent Operational Requirements procedure, given that these systems were not deployed on the basis of long-term capability development, but rather because of immediate operational necessity. It is therefore not entirely clear, according to the document, what will happen to these systems after the end of the operation in Afghanistan, following the withdrawal of forces, and which authority will be responsible for developing a comprehensive, force-wide guidance on this issue. Regardless of future acquisitions, it will be necessary to determine what future capabilities unmanned aerial vehicles may represent and how their deployment will impact on the organisations that use them. The doctrine also points out that if we look at unmanned aircraft as a system, and take into account their ever-expanding range of increasingly modern and thus much more expensive technical equipment, the value for money is not as attractive, at least compared to piloted aircraft. According to the 'Defence Equipment Plan 2012' published in January 2013, the UK Ministry of Defence plans to spend around Â£18.5 billion over the next 10 years on developing air combat capabilities, with a particular emphasis on the procurement and development of unmanned aerial assets. A striking example of the UK's ambition is the UK-France agreement in July 2012 to develop a joint Future Combat Air System. Furthermore, the MoD confirmed in May 2012 that it was in talks with the US Government to develop a joint programme with the UK for the X-47B unmanned aerial demonstration system cooperation. The UK is also involved in the development of the Neuron Unmanned Combat Air Vehicle, in which several other European countries (France, Greece, Italy, Spain, Sweden and Switzerland) are also involved.

3.Working Party 29 recommendation

The European Union's Working Party on Data Protection 29 adopted its opinion at its meeting in June 2015. [24] The opinion argues for the importance of specific regulation of drones at European level as well as at national level. The opinion supports any solution that promotes transparency and facilitates the exercise of data subjects' rights by identifying the data controller. It also stresses the responsibility of manufacturers to enforce data protection requirements. In this context, the principle of privacy by design should be emphasised, which imposes a requirement on the actors to take into account the privacy impact of technology at the design stage. As designers and manufacturers are the first to be able to influence the subsequent use of the technology, this is why the document highlights the importance of this principle. Like the privacy by default principle, the new reform package brings the former principle to the level of a regulation. Working Party 29 does not consider it necessary that a law should be the legal basis for data processing by drones. It believes that the issue should be approached from the point of view of the different purposes for which it is used. This means that, in addition to the so-called mandatory processing based on

law, other legal bases in the EU Data Protection Directive could also be considered for the use of UAS. This kind of differentiated approach would thus allow more scope for weighing the interests at stake on a case-by-case basis. In my opinion, alongside drones, self-driving cars are another priority target of cyberterrorism, including cyberattacks, in the 21st century. My assertion is borne out by the terrorist attacks by numerous suicide bombers in vehicles that have shaken the world. That is why I felt it was important to address it in my thesis.

4. Self-driving cars

In the 21st century, we are increasingly seeing cars that are computer-controlled or have some form of computer-network connection, including increasingly wireless network access and data transmission. Electronic immobiliser, tyre pressure monitoring or even ABS systems are now standard features of today's cars, but more modern cars also have wireless entertainment systems, to which we can connect our smart phones wirelessly, or even systems that recognise traffic signs, not to mention intelligent navigation. The Internet of Things is also coming to cars, with the systems that are increasingly are increasingly emerging with extended functions, the ability to communicate with each other and to perform various interventions in physical space.[25] Self-driving cars have also appeared on the road. The first and most famous example is Tesla. Tesla's entry into the car market has created a competitive situation in the industry that the major car manufacturers could not and do not ignore. Tesla has brought a number of innovations into the public domain, mainly based on information technology. However, there is a problem with the electronics and computer systems in cars. Paradoxically, this problem is precisely a safety issue. In 2014, two young researchers - Charlie Miller and Chris Valasek - examined nearly twenty cars of different types manufactured between 2006 and 2014, analysing their wireless connections.

The researchers identified at least 20, and in some cases close to 100, data transmission links (electronic control units and their interconnections) and solutions per car that were used wirelessly by the vehicles studied for their various functions. [26] The two researchers have analysed and tested in practice the solutions to access and manipulate the various systems or even cyber-physical subsystems of the car through these wireless links. [27] The authors divided these attacks into three phases or access solutions. In the first stage, the attacker gains remote access to the car's systems, allowing him to send messages to the car's various networks, so that he can directly or indirectly control the electronic control unit. However, in many cases this type of intervention can only be successful if it exploits a vulnerability in a system. . One example is the known vulnerability of Bluetooth, which has already been used by researchers at the University of Washington and the University of California San Diego to remotely access a vehicle's telematics units. However, the study summarising the results of this study concludes that a cyber-physical attack usually requires a second step, because the electronic control units that can be accessed remotely in the first step are not capable ofdirectly controlling the physical intervening units. The third step is to inject fake control commands into the critical systems, which is only a seemingly simple task because different vendors use different data structures, so successful intervention or code execution requires first analysing them.

The study also looks at possible conservation solutions The first such protection solution is to reduce or close the attack points, the services that can be remotely controlled. Another important protection issue is to improve the vulnerabilities of related services, such as the aforementioned Bluetooth, or to properly encrypt network traffic, making it more difficult to easy code execution for attackers. In 2016, four Chinese cybersecurity researchers - Samuel LV, Sen Nie, Ling Liu and Wen Lu - demonstrated in a spectacular demonstration that Tesla's systems can be hacked from several kilometres away. During the test, the researchers were able to move the car's electrically adjustable seats, open the sunroof and boot, or even control the instruments from 12 miles away via the Tesla Model S CAN bus, while the car was in drive mode. In its official response, Tesla of course tried to downplay the issue, because it believes that this kind of remote system access is only possible in Tesla vehicles when the on-board computer is running a web browser and the car is close to a wifi hotspot that has been compromised, i.e. hacked, and through which an attack could be carried out. [28]

In May 2016, the University of South Carolina, Zhejiang University in China and the Chinese security company Qihoo 360 intervened in Tesla's Autopilot electronic system, which allows the car to drive automatically, by creating non-existent obstacles that Autopilot thought were real. It follows that cybersecurity in the field of cars with network connectivity and internet access is as important an area as the various systems that create and enhance physical security in cars. Looking to the future, safety should be even more of a priority in this area, as it is already predicted that in the future we will be driving cars that are not driven by humans but by computers with built- in artificial intelligence.

As we recently learned in the case of the Uber self-driving car fatality, testing self-driving vehicles comes with a lot of responsibilities and risks. With that in mind, I want to look at the rules and licensing requirements in the US that a company must comply with if it wants to test its own self-driving vehicle on the road. In the absence of federal regulation, the legal framework for road testing of self-driving cars was initially determined by the individual states, with the result that completely different requirements were established in the states and different criteria had to be met for each vehicle. As a consequence, the movement of self-driving cars between States was a legal nightmare. In order to harmonise the heterogeneous regulations, the US National Highway Traffic Safety Administration ("NHTSA") stepped in and created the Federal Automated Vehicles Policy in September 2016. NHTSA later revised it and created "Automated Driving

Systems: A Vision for Safety 2.0. This guidance consists of two major sections: the first provides guidance to companies on the road in traffic for and the second advises the states on their local legislative responsibilities. [29] NHTSA also settles, in a soft law manner, issues that have arisen in relation to federal and state responsibilities. Under NHTSA's guidance, federal jurisdiction includes the regulation of safety standards and public training, while the issuance of driver's licenses, enforcement of statutory requirements, and the issuance of testing permits remain state responsibilities. Only after meeting the 12-point set of requirements set by the NHTSA can self-driving vehicles developed by companies be road-tested. The aforementioned set of requirements covers areas such as continuous documentation during operation, cyber security, object and event detection and self-driving system security. If a company's self-driving vehicle meets all the requirements, all that remains is to obtain approval in the relevant state(s). If it is found to be in compliance, the licence will be issued by that state. The NHTSA has committed in its guidelines to update the document from time to time, so it remains to be seen whether the federal agency will tighten or clarify after the Uber-related fatal accident. Among other reasons, the regulation of self-driving vehicles on the roads is important because it can attract companies developing this technology to the state if the right regulatory conditions are in place. The growing attention to self-driving vehicles and their increasing participation in road traffic clearly shows that there is a strong pressure on legislators to ensure the right conditions, to create a uniform regulatory environment and to build up citizens' confidence in self-driving vehicles.

5. Cyber security in NATO

In 2007, an incident in Estonia caused a serious political and strategic dilemma in NATO. This was mainly because it was the first cyber-attack in the Alliance's history - not in the physical dimension - that drew attention to the dangers of cyberspace and to a new era. One of the most relevant elements in the 21st century is cyberspace itself, or rather the reality that a country can no longer be attacked not only in the previously well-defined and relatively well-characterised traditional dimensions (land, air, sea, space) but also through the new dimension of cyberspace. In the Alliance, this recognition led to the inclusion of the task of protecting military intelligence and information systems in the strategic concept of the organisation after the 2010 NATO Summit in Lisbon (NATO 2010). Fortunately, the strategic thinking on cyber threats among NATO decision-makers did not stop there, as on 8 June 2011, the defence ministers of NATO member states signed the the Alliance's new cyber defence policy. This document not only contained a strategic vision for cyber defence, but also an action plan, the detailed programme of which was adopted in October 2011. In February 2012, the full deployment of the NATO Cyber Incident Response Capability (NCIRC) was launched, along with the establishment of a Cyber Threat Awareness Cell.[25] The biggest step forward in cyberspace was the Warsaw Summit in 2016, when the Alliance officially declared cyberspace as an operational dimension. Cyberspace thus officially became a warfighting dimension. As this is a defining event in the Alliance's thinking on cyberspace, it is useful to quote the relevant part of the official NATO statement: 'Cyber-attacks are clearly a challenge to Alliance security and can be as damaging to modern societies as traditional attacks. Now in Warsaw, we are reaffirming NATO's defence mandate and recognising cyberspace as an area of operations in which NATO must defend itself as effectively as in the air, on land and at sea."[30]

6. Results

I have referred to the complex areas of cybersecurity and information security several times in the chapters of this thesis. It is clear that each of these areas is of such a large scale that it is not possible to cover them in their entirety in the context of a single essay. After the considerations that I have set out in my thesis, I must now turn to the complex understanding of information security and its implementation in an organisation, which paradoxically does not begin with the establishment of a defence but - de lege ferenda - with a document. And this document is nothing other than the information security policy of a given State and a given organisation. In practice, it is a short but clear and understandable statement of the commitment of the leadership of the state to security. This policy also includes an expression of which components as the most important factor to protect and what is being done to ensure that this is the case. A Documents are prepared taking into account the information security principles of confidentiality, integrity and availability, and include not only the definition of physical, administrative and logical protection measures, but also the provision of the necessary material and human resources. In my opinion, the document should contain the following elements.

It is possible for someone to become a participant through negligence, for example by neglecting to protect their own computing devices, making their computer a zombie in such an operation. Obviously, in this case, the person cannot be considered an active participant in the absence of intent, and the victim cannot decide whether the device he is operating is a deliberate or negligent participant in the attack against him. This problem points to the second point that the document should include, which is awareness. The safe use of infocommunication tools and the Internet must be taught. Every day, dozens of new threats and challenges are faced by anyone who goes into cyberspace, and the user must be prepared for

them. It follows that cybersecurity education should be included in the National Curriculum. In addition to user- level IT skills, cybersecurity issues should be taught and their theoretical application in practice should also be started in public education. The third element, in my opinion, must be the regulation of drones and self- driving cars and a number of smart devices, in accordance with the law of technology, because until these areas are regulated, the operating platform for cyberterrorism will continue to expand. I cannot state unequivocally that the international documents we currently have are not sufficient to assess cyber-attacks, but I am convinced that a single document, at least within NATO, - which would include the 3 points taken up in this chapter - would certainly facilitate the international legal assessment of cyber-attacks and the possible application of a 'procedure', but above all the fight against cyber-attacks.

REFERENCE

1.UN Charter Article 51
2.FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95. § 331(9)
3.AIR 160: Interim Operational Approval Guidance 08- 01 of the Aviation Safety Unmanned Aircraft Program Office of the FAA on Unmanned Aircraft Systems Operations in U.S. National Airspace System, 13 March 2008.https:// papers.ssrn.com/sol3/papers.cfm?abstract_i d=2763374
4.SHARKEY Noel: Saying 'No!' to Lethal Autonomous Targeting Journal of Military Ethics, 2010.(4) 369- 383.
5.SULLIVAN Sean: Domestic Drone Use and the Mosaic Theory University of New Mexico School of Law Legal Studies Research Paper Series, Paper No. 2013-02 1.
6.GAO-12-981: Report of the U.S. Government Accountability Office on Unmanned Aircraft Systems - Measuring Progress and Addressing Potential Privacy Concerns would Facilitate Integration into the National Airspace System, September 2012. http://www. gao.gov/assets/650/648348. pdf
7.SWD(2012) 259 final: Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS), Brussels, 6 September 2012.
8.Lászlóné Siska Katalin Szűcs: International Law - UNIVERSITAS-GYŐR Nonprofit Ltd. (2023) - 298.
9.SINGER, Peter W. -STAUCH, Günther -BUCK, Christian: Mords -machines -Technology Review Heise Zeitschriften Verlag (May, 2012), pp. 28 -34.
10.Dr. Lászlóné Dr. Katalin Siska Szűcs: The reforms of Kamál Atatürk in the light of the contemporary Hungarian press and the pro-government Turkish cumhuriyet - Debrecen University Press (2020) - 241.
11.Dr. Lászlóné Dr. Katalin Siska Szűcs - The limits of fundamental rights and the practice of the specific assessment of the public interest in Turkey - Digitall Sapiens Ltd. (2023) - 10.
12.Katalin Siska: Family law provisions in modern Turkey, with special regard to the substantive and procedural issues of mixed marriages; In: Jog, Staat, politika. 14 (1), 143-160, 2022.
13.Katalin Siska: The impact of Mustafa Kemal Atatürk on the concept of Turkish identity and citizenship, with special regard to constitutional law - In: Law, State, Politics Vol.8 No.1 (2016) - 61.
14.KOLESZÁR Béla: Ethical issues of robot warfare II Military morality In: Military Engineer, Vol. V No. 1 (March 2010), pp. 266-283.
15.MAURIELLO Tracie: Do drones make killing and spying too easy http://www.postgazette.com/stories/news/world/do-drones- make-killing-spying-too-easy-633606/
16.ALTMANN Jürgen: Preventive Arms Control for Uninhabited Military Vehicles In: R. Capurro and M. Nagenborg (Eds.), Ethics and Robotics, AKA Verlag Heidelberg (2009), pp. 69 - 82.
17.MATT J Martin - SASSER Charles W.: Predator: The Remote Control Air War over Iraq and Afghanistan: A Pilot's Story - Zenith Press (2010) -ISBN: 978-0-760- 3896 -4, 310.
18.OUDES Cor - ZWIJNENBURG Wim: Does Unmanned Make Unacceptable? Exploring the Debate on using Drones and Robots in Warfare -IKV Pax Christi (May 2011) - ISBN: 9789070443672, 39 p.
19.SPARROW Rob: Robotic Weapons and the Future of War In: Jessica Wolfendale and Paolo Tripodi (eds): New Wars and New Soldiers: Military Ethics in the Contemporary World - Ashgate Publishing, Ltd. (2011), pp. 117 -133. - ISBN: 9781409401056, 281.
20.LIN Patrick - BEKEY George - ABNEY Keith: Autonomous Military Robotics: Risk, Ethics, and Design CALPOLY, US Department of Navy, Office of Naval Research (December 20, 2008) http:// ethics.calpoly.edu/ONR_report.pdf
21.Autonomous Vehicles in Support of Naval Operations - Committee on Autonomous Vehicles in Support of Naval Operations, National Research Council National Academies Press https://nap.nationalacademies.org/catalog/11379/ autonomous -vehicles-in-support-of-naval-operations
22.Unmanned Systems Integrated Roadmap FY2011 -2036 - USA Department of Defence, Ref.No. 11-S- 3613
18. The UK Approach to Unmanned Aircraft Systems, Joint Doctrine Note 2/11 - Ministry of Defence, Development, Concepts and Doctrine Centre (30 March 2011)-https:// assets.publishing.service.gov.uk/media/5a81d239ed91 5d74e34003bc/20110505-JDN_2-11_UAS_archived-U.pdf
23.WP 231: Opinion 01/2015 of the Article 29 Working Party on Privacy and Data Protection Issues relating to the Utilisation of Drones, 16 June 2015 https://ec.europa.eu/ justice/article-29/documentation/opinion- recommendation/index_en.htm
24.NIST Cyber-physical System (2017): NIST Cyber-physical System. https://www.nist.gov/el/cyber-physical-systems/cyber-physical-systems
25.VALASEK Chris - MILLER Charlie (2014): A Survey of Remote Automotive Attack Surfaces. www.ioactive.com/pdfs/IOActive_Remote_Attack_Surfaces. pdf.

26.ICS-CERT (2017): Alert (ICS-ALERT-17-209-01) CAN Bus Default Vulnerability https://www.cisa.gov/news-events/ics-alerts/ics-alert-17-209-01
27.SOLON Olivia (2016): Team of Hackers Take Remote Control of Tesla Model S from 12 Miles Away. The Guardian, 2016. 09.20.https://www.theguardian.com/technology/2016/sep/20/tesla- model-s-chinese-hack-remote-control-brakes
28.http://www.nhtsa.gov/manufacturers/automated-driving- systems
29.NATO (2017): Cyber Defence. https://natolibguides.info/cyberdefence/reports
30.NATO (2016): Warsaw Summit Communiqué www.nato.int/cps/en/natohq/official_texts_133169.htm