ACTA IURIDICA RESOVIENSIA Nr 4(43)/2023
ISSN 2720-0574 DOI: 10.15584/actaires.2023.4.4

Robert Łasa

University of Silesia in Katowice
ORCID: 0000-0001-6257-3371

MILITARY REVIEW IN THE CONTEXT OF CYBER-WARFARE. ARTICLE 36 OF 1977 ADDITIONAL PROTOCOL I IN PRACTICE

Introduction

This study aims to identify problems in controlling the legality of the means and methods of cyber-warfare. Nowadays, military actions in cyberspace are not uncommon. On the contrary, states report the creation of the new means of cyber-warfare, which are regularly used for operations in the Net.

The main research problem is the implementation of military review stipulated in Art. 36 of the 1977 Additional Protocol I (AP I) in the context of cyberweapons, means and methods of warfare. The research recognised specific problems: how is a cyber-attack defined in the context of international humanitarian law? how should the legality of means and methods of cyberwarfare be controlled? what is the practice of states in this regard?

The research's primary method is the dogmatic one, which renders it possible to analyse the norms of international humanitarian law (IHL) in terms of treaties and customary law. A complementary role is played by the theoretical method, which indicates the position of the doctrine and of states and international organisations, including such as ascertained by analysing their official documents.

Cyber-attack in an armed conflict

Although a cyber-attack is no longer an entirely new means or method of warfare, it still poses many problems in terms of definition and legal regulation.

It is difficult to identify one precise definition of a cyber-attack. It mainly depends on its context, i.e., whether it is an attack in peacetime against state institutions or private companies the perpetrators of which are often hackers not

connected with any state authority motivated only by profit or gaining access to information, or, perhaps, a cyber-attack against another state (starting an armed conflict). The considerations of this paper will focus on cyber-attacks in the context of an armed conflict. The cyber-attack can be defined narrowly as operations that cause damage to people or objects or, in a broader sense, as the functionality of objects and facilities that can be used during an attack[1]. One of the main definitions of a cyber-attack has been created by the International Group of Experts (the IGE) forming the Tallinn Manual[2], according to which the cyber-attack is a cyber operation, either offensive and defensive, causing injury or death to persons, or damage or destruction to objects[3]. By analysing the formulated definition, the three essential characteristics of the cyber-attack can be identified:

– it is an act of violence,
– it has a specific purpose,

and

– it has an offensive or a defensive character.

Another primary concern is the lack of legal norms relevant to cyberattacks during an armed conflict. Currently, no international agreement regulates this matter, mainly, due to the lack of political will on the part of states. The lack of regulations in this regard acts to the advantage of attackers as it is more difficult to determine the legality a cyber-attack or the lack of it. Despite these doubts, states, on the basis of the treaties and customary law, are still obliged to conduct the military review of every weapon, means and method of warfare.

The purpose of military review

The basic principle in the choice of means and methods of warfare in the course of an armed conflict is that the parties to the conflict do not have an unlimited selection of means of warfare (see Art. 35 of AP I)[4]. Unquestionably, this is one of the oldest principles governing the manner of an armed conflict. As early as the 17th century, Grotius indicated the need to limit the destructive power of specific weapons[5].

[1] V. Boulanin, M. Verbruggen, *Article 36 reviews: Dealing with the challenges posed by emerging technologies*, Solna 2017, p. 11.

[2] M.N. Schmitt, *Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations*, Cambridge 2017.

[3] *Ibidem*, p. 415.

[4] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, 1125 UNTS 3.

[5] C. Pilloud, J. de Preux, Y. Sandoz, B. Zimmermann, P. Eberlin, H.P. Gasser, C.F. Wenger, S.S. Junod, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Geneva 1987, par. 1383.

A milestone was the Hague Regulations of 1907, which reiterated this principle in Art. 22, granting it treaty status[6].

Restriction in the choice of the means and methods of warfare is intended to eliminate such weapons (but also tactics and methods of the conduct of hostilities) that would cause not only suffering among combatants or civilians, but also damage to the environment (see Art. 35(2) of AP I) from the arsenal of the parties to an armed conflict.

States are obliged to adopt suitable measures to bring armaments into compliance with the requirements of Art. 35 of AP I. The answer to the question of what these measures are to be is Art. 36 of AP I, which imposes the obligation of so-called military review (legality control). It means that the state, at each stage of the selection of a particular type of armament and possible inclusion of it in its arsenal, must examine, whether the use of that armament is not prohibited *per se* or whether using it in a specific manner will not violate IHL (see Art. 36 of AP I).

Military review is a mechanism at the border of IHL and arms control law. The obligation to control the legality of armaments mainly falls during peacetime when states are developing their military capabilities. Not only do IHL norms affect the activities of states only during an armed conflict, but also require them to act accordingly during peace. Although the measures taken are intended to eliminate the harmful effects of armed conflicts such as unnecessary suffering or superfluous injury, it is essential to note the impact of military review on arms control and disarmament issues[7]. Effective military review eliminates armaments prohibited by IHL, and, thereby, it can be expected that, in the future, such armaments will be removed entirely from the arsenal of any state, and that this step will contribute to disarmament.

To properly define the scope of military review, it is necessary to invoke the instruction drawn up by the International Committee of the Red Cross (the ICRC Instruction)[8], which specifies, among other things, the catalogue of weapons subject to review:

- weapons of all types,
- how these weapons are to be used according to military doctrine, tactics, the rules of engagement, operating procedures and counter-measures,
- all weapons to be acquired, be they procured further to research and development based on military specifications or purchased 'off-the-shelf',

[6] Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 18 October 1907, 36 Stat. 2277.

[7] A. Dienelt, *The Shadowy Existence of the Weapons Review and Its Impact on Disarmament*, Sicherheit und Frieden (S+F)/Security and Peace 36, 3, 2018, p. 131.

[8] ICRC, *Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, International Review of the Red Cross 88, 864, 2006.

– a weapon that the state intends to acquire for the first time, without necessarily being 'new' in a technical sense,
– an existing weapon that is modified in a way that alters its function, or a weapon that has already passed a legal review, but is subsequently modified,
– an existing weapon where a state has joined a new international treaty which may affect the legality of the weapon[9].

Therefore, states are obliged to review under Art. 36 of AP I. The issue is the identification of the necessity of military review as a customary law norm. The doctrine assumes that military review has not developed into a customary law norm so far[10]. The opponents of this theory indicate that some of the major military powers, the United States (US) and Israel, even though they are not parties to AP I, conduct military review as part of their military activities[11]. Undoubtedly, this is evidence that arms legality control may become a customary norm, but it cannot be stated clearly. This is due, among other things, to the lack of a unified regulation of what such a review should look like, but there is also the lack of information on how often states conduct this review[12]. The issue of military review as a potential customary norm was analysed during the IGE's work on the Tallinn Manual 2.0[13]. In the first place, experts formulated a rule according to which states are obliged to ensure that their means and methods of warfare comply with IHL[14]. The implication would be that a state could introduce some substitute for military review to implement the obligation in Art. 36 of AP I sufficiently[15].

The opposite stance was advocated in the ICRC Instruction. At its very beginning, it was indicated that military review is not a new concept, and that its history dates back to the 19th century[16]. The argument for the customary nature of military review is based on international treaties regulating the means and methods of warfare[17]. Unfortunately, this is a mistaken approach because the cited conventions relate to states' restrictions on using particular types of weapons. At the same time, none of them imposed an obligation to review weapons. The control of legality in the perspective of the customary norm could originate in the Martens Clause, which would permit the use of weapons under the principle of humanity and the requirements of human conscience[18].

[9] *Ibidem*, pp. 937–938.

[10] N. Jevglevskaja, *Weapons Review Obligation under Customary International Law*, „International Law Studies" 2018, No. 94, p. 213.

[11] *Ibidem*.

[12] *Ibidem*, p. 209.

[13] *Ibidem*, p. 215.

[14] M.N. Schmitt, *Tallinn Manual 2.0*…, p. 464.

[15] N. Jevglevskaja, *Weapons Review*…, p. 215.

[16] ICRC, *Guide to the Legal*…, p. 932.

[17] *Ibidem*, pp. 941–942.

[18] V. Boulanin, M. Verbruggen, *Article 36 Reviews*…, p. 17.

Military review procedure

At present, there are no legal regulations relating to what military review should look like. An example of the procedure is described in the ICRC Instruction. As a general rule, the duty to review weapons rests with the authority responsible for matters related to national defence[19]. Within these institutions, a department or other unit responsible for legal services is created, and legal advisors work in it (see Art. 82 of AP I).

The vital matter is to determine when a review should take place. Article 36 of AP I does not give any directions in this regard, while it should be assumed that the review should take place at the earliest possible stage, whether it be research work or as early as the time of the arms purchase. It is assumed that the review should take place at the time of design for a state that produces weapons[20]. In contrast, for a state that decides to purchase the weapon, the review should occur at the time of reviewing the offer[21].

A controversial issue is the state's ability to keep the information whether or not the weapons meet the criteria of legality in secret. Information, whether the weapon is illegal *per se* or its use in a particular case could be unlawful is not required to be made public[22]. It is up to the state to decide, whether to provide such information to other states and what issues can remain undisclosed even further. Despite the lack of clear regulations on making the results of military reviews public, most states publish reports so that knowledge is widely available, which positively affects the transparency of IHL[23]. Based on Art. 84 of PD I, attention has been repeatedly drawn to the need to share information on how military reviews are conducted[24].

Cyber military review

On numerous occasions, it is claimed that IHL is not adapted to the challenges raised by the modern means and methods of warfare. To some extent, it is impossible to disagree with this, given that AP I was drawn up in the 1970s.

[19] ICRC, *Guide to the Legal*…, pp. 949–950.

[20] *Ibidem*, p. 951.

[21] *Ibidem*, p. 952.

[22] C. Pilloud, J. de Preux, Y. Sandoz, B. Zimmermann, P. Eberlin, H.P. Gasser, C.F. Wenger, S.S. Junod, *Commentary on the Additional*…, par. 1481.

[23] L. Wexler, *International Humanitarian Law Transparency*, „Illinois Public Law Research Paper" 2013, No. 14–11, p. 16.

[24] *Declaration Agenda for Humanitarian Action Resolutions*, 28th International Conference of the Red Cross and Red Crescent Geneva, 2–6 December 2003, p. 20.

However, it is essential to note the universal nature of Art. 36 of AP I and that it is entirely in line with the changes in the modern means and methods of warfare. This was also the assumption of the authors of AP I[25].

Military review must also include means and methods related to a possible armed conflict in cyberspace. Weapons that could be used to attack in cyberspace should be controlled under the mechanism provided for in Art. 36 of AP I[26], thereby, excluding weapons that violate IHL norms and principles.

Consideration should focus on the potential consequences of a cyber-attack . Those responsible for conducting the review should weigh, whether a possible cyber-attack could cause harm to civilians (damage visible in the physical world such as the loss of health or death), but also, whether it could lead to the physical loss or destruction of data (by which all and any data necessary for the proper functioning of civilian facilities that facilitate the protection of civilians are meant)[27]. Given the growing interest in environmental protection, including in the context of an armed conflict, military review should verify that a cyber-attack would not cause widespread, long-term and severe damage to the environment[28]. A potential cyber-attack should also be checked in the context of the prohibited methods of warfare, including perfidy, the purpose of which is to mislead the adversary, thereby, depriving him of the protection provided by IHL (see Rule 122 of the Tallinn Manual 2.0 and Art. 37(1) AP I).

The obligation under Art. 36 of AP I applies to the potential violations of IHL. Therefore, while reviewing the legality of weapons, means and methods of warfare, a state should consider potential issues of violating the neutrality of third countries in an armed conflict. Network interconnections mean that the cyber-attack using a computer network, specifically the Internet, can violate the neutrality of third countries[29]. In an advisory opinion on the legality of the threat or use of nuclear weapons, the ICJ stated that neutrality is one of the fundamental principles of international law and should be respected in the course of an armed conflict on par with IHL principles as part of customary law[30]. As the cyber-attacks that have already been conducted show, the violation of a third country's network, and thus the violation of its neutrality, is something familiar aimed at rendering it more difficult to detect the perpetrators of these attacks

[25] C. Pilloud, J. de Preux, Y. Sandoz, B. Zimmermann, P. Eberlin, H.P. Gasser, C.F. Wenger, S.S. Junod, *Commentary on the Additional*…, par. 1478.

[26] M.N. Schmitt, *Tallinn Manual 2.0*…, p. 464.

[27] V. Boulanin, M. Verbruggen, *Article 36 Reviews*…, p. 14.

[28] *Ibidem*.

[29] M. Roscini, *Cyber Operations and the Use of Force in International Law*, New York 2014, p. 259.

[30] Legality of the Threat of Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996, 226 (8 July), par. 88–89.

(also by changing the IP for another corresponding to a country not being an actual attacker)[31].

The expected military review should consider another issue that has not been of much importance so far due to the lack of or limited capabilities to seize enemy weapons remotely. If the cyber-attack was to seize a specific model of an adversary's weapons, military review should also consider the legitimacy of the weapons being seized[32].

Following the stance of M.N. Schmitt, the above can be summarised in four main questions that the results of the legality check should answer[33]. First, in the regular use of a means or method of warfare, would its purpose be to cause unnecessary suffering? Second, would the use of a means or method of warfare cause an attack to be conducted without distinction (indiscriminate nature)? Third, could the use of a means or method of warfare result in a violation of international law? Fourth, are adequate legal norms regulating the means and methods of warfare in cyberspace in place? The answers to these questions will render it possible to take appropriate steps to eliminate certain weapons from the state's arsenal, limit their use in specific cases, or allow their full use. While the issues of complete prohibition or full use of the cyber methods and means of warfare do not raise significant questions, it is necessary to identify possible ways to limit them[34]. First of all, the target of an attack should be specifically designated, which is supported by the principle of distinction and the law of targeting, i.e. norms that determine how a state should aim at particular persons or objects. In addition, the issue of using cyber means of warfare in a specific way such as using a particular network, thus preventing the violation of the neutrality of third countries, should be analysed. If the malware spreads to other targets not planned initially, a cyber-weapon should be able to self-destruct. This will render it possible to control the attack, thus reducing the potential possibility of its loss.

States' practice in military review

Nowadays, it is possible to notice a trend towards conducting more frequent military reviews, especially, in the context of the means and methods of cyber-warfare. A key role in spreading military review is played by the US. According to instructions imposed by the U.S. Department of Defense, every new weapon must be subject to a legality review. The review must answer the following questions:

[31] *China IP address link to South Korea cyber-attack*, https://www.bbc.com/news/world-asia-21873017 (6.09.2023).

[32] V. Boulanin, M. Verbruggen, *Article 36 Reviews*…, p. 14.

[33] M.N. Schmitt, *Tallinn Manual 2.0*…, pp. 466–467.

[34] V. Boulanin, M. Verbruggen, *Article 36 Reviews*…, p. 14.

whether the weapon's intended use is calculated to cause superfluous injury? whether the weapon is inherently indiscriminate? whether the weapon falls within a class of weapons that has been specifically prohibited?[35] Moreover, the United States conducts a two-step review of the legality of means and methods of warfare. First, it examines whether the use of such a means or method of warfare would not be prohibited *per se*, and then it examines the use of that means or method of warfare already in a specific operation[36]. The US Air Force was among the first to start requiring the review of the means and methods of cyberwarfare due to their destructive nature[37]. In addition to the practice, attention should be paid to the positions of states that have committed to such a review.

Canada confirmed that all AP I parties must conduct military reviews in the context of cyber operations, even if these did not involve any means or method of warfare[38]. A similar position was taken by Switzerland, which also confirmed that AP I parties are obliged to conduct military review, including the means and methods of warfare that could assist in cyber operations[39].

According to the Australian government's official position, Art. 36 of AP I requires states being parties to the agreement determine, whether the use of new weapons, means or methods of warfare would be prohibited in some or all circumstances. In addition, cyber preparedness (the ability to conduct military activities in cyberspace) may, under certain circumstances, constitute a weapon, means, or method of warfare within the meaning of Art. 36 of AP I[40]. A similar position was taken by the Brazilian government, adding that**,** although the norm of Art. 36 of AP I is not as stringent as some states would like it to be, it still contains sufficient elements to perform a preventive function[41].

---

[35] USA, Department of Defense, *Law of War Manual*, June 2015 (Updated December 2016), https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190 (19.11.2023).

[36] *International Law in Cyberspace*, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm (19.11.2023).

[37] D. Wallace, *Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis*, „Tallinn Paper" 2018, No. 11, p. 15.

[38] *International Law applicable in cyberspace*, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng (6.09.2023).

[39] *Switzerland's position paper on the application of international law in cyberspace*, https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf (6.09.2023).

[40] *Australia's submission on international law to be annexed to the report of the 2021 Group of Governmental Experts on Cyber*, https://www.internationalcybertech.gov.au/sites/default/files/2021-06/Australia%20Annex%20-%20Final%2C%20as%20submitted%20to%20GGE%20Secretariat.pdf (6.09.2023).

[41] *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by*

The German government considers military review as one of the possible complementing precautions in an armed conflict. The results of arms legality control should form the basis of preparing military operations. This implies that the development and adoption of the means and methods of warfare will often coincide with planning a specific operation[42].

One of the most recent positions was presented by Costa Rica. In July 2023, the Costa Rican government confirmed that all states, due to the customary nature of the military review, are required to implement the review in the context of new means and methods of warfare, including cyber means and methods of warfare[43]. The government has indicated that the review would include verifying the legality of malicious malware, e.g. ransomware.

Cyber-attacks in practice

Even though cyber-attack is one of the newest means of conducting operations in armed conflict, it is counterintuitively not used very often. Leading the way here is the Russian Federation, which has been using cyber-attacks in every conflict in which it participates for more than 15 years.

The 2007 attack on Estonian government offices and institutions, such as banks, should be identified as one of the first Russian cyber-attacks[44]. Although it occurred in peacetime and was not linked to an ongoing armed conflict it represents a stepping stone to military operations conducted in cyberspace. The entire campaign lasted as long as 22 days, during which official websites were attacked, denying public access to them. The genesis of the attacks seems rather prosaic, as the Estonian government wanted to move a monument to Soviet soldiers from the center of the capital to a local military cemetery. This sparked outrage among Estonia's Russian minority, leading to riots. Less than a year later

participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, 13/07/2021, UN Documents A/76/136, p. 23.

[42] Federal Government of Germany, *On the Application of International Law in Cyberspace*, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf (6.09.2023).

[43] *Costa Rica's Position on the Application of International Law in Cyberspace*, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf, UNODA Library (19.11.2023).

[44] R. Ottis, *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*, Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth 2008, p. 163.

there was an armed conflict between Russia and Georgia[45]. The Russians, with the help of private companies supported by the intelligence service, conducted an extensive campaign to limit Georgia's cyber capabilities[46].

The Russians have also been active in Ukrainian cyberspace since the annexation of Crimea in 2014[47]. They were already actively attacking Ukrainian critical infrastructure facilities in the early years of the conflict – the power grid in the Ivano-Frankivsk region in 2015[48] and a power plant in Kiev in 2016[49]. Since the full-scale invasion of Ukraine, the Russians have also conducted extensive cyber operations. However, unlike previous attacks, the current focus is mainly on cyber-espionage and cyber-attacks of a disruptive nature[50].

Conclusion

To eliminate unnecessary suffering during an armed conflict, the international community has decided to build a mechanism controlling the legality of weapons even before they are used. Unfortunately, military review has not been sufficiently regulated by law, which results in gaps in its execution.

The main problem is the lack of legal norms indicating who or what institutions are responsible for conducting arms reviews. Should these be lawyers employed in the legal departments of the defence ministries or the general staff? Should a unique international organisation be established to control the legality of the weapons of the state parties, including by analysing annual reports? What is also questionable is the lack of reports on the review's outcome, mainly, if the weapons were found illegal.

States should be interested in conducting military reviews primarily from the perspective of IHL functions such as excluding unnecessary suffering and protecting the environment during an armed conflict or the principle of distinction. On the other hand, if such arguments do not persuade them, they should approach

[45] M. Rzeszuta, *Sieć. Piąty Teatr Działań Wojennych: 2008 – Informatyczna Blokada Gruzji*, „Układ Sił" 2020, No. 23, p. 52.

[46] P. Shakarian, *The 2008 Russian Cyber Campaign Against Georgia*, „Military Review" 2011, November–December, p. 63.

[47] G.B. Mueller, B. Jensen, B. Valeriano, R.C. Maness, J.M. Macias, *Cyber Operations during the Russo-Ukrainian War From Strange Patterns to Alternative Futures*, Center for Strategic and International Studies, 13 July 2023, p.5.

[48] *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case*, Electricity Information Sharing and Analysis Center, Washington D.C. 2016, p. IV.

[49] *Ukraine's power outage was a cyber attack: Ukrenergo*; https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA (19.11.2023).

[50] G.B. Mueller, B. Jensen, B. Valeriano, R.C. Maness, J.M. Macias, *Cyber Operations*…, pp. 7–8.

the issue of reviews more pragmatically; that is, eliminating illegal weapons at the very beginning of researching them or at the time of verifying a bid will save significant sums in the state budget, which would otherwise be used for further research or negotiations.

Bibliography

Boulanin V., Verbruggen M., *Article 36 reviews: Dealing with the challenges posed by emerging technologies*, Solna 2017.

Dienelt A., *The Shadowy Existence of the Weapons Review and Its Impact on Disarmament*, Sicherheit und Frieden (S+F)/Security and Peace 36, 3, 2018.

Jevglevskaja N., *Weapons Review Obligation under Customary International Law*, „International Law Studies" 2018, No. 94.

Mueller G.B., Jensen B., Valeriano B., Maness R.C., Macias J.M., *Cyber Operations during the Russo-Ukrainian War From Strange Patterns to Alternative Futures*, Center for Strategic and International Studies, 13 July 2023.

Ottis R., *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*, Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth 2008.

Pilloud C., de Preux J., Sandoz Y., Zimmermann B., Eberlin P., Gasser H.P., Wenger C.F., Junod S.S., *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Geneva 1987.

Roscini M., *Cyber Operations and the Use of Force in International Law*, New York 2014.

Rzeszuta M., *Sieć. Piąty Teatr Działań Wojennych: 2008 – Informatyczna Blokada Gruzji*, „Układ Sił" 2020, No. 23.

Schmitt M.N., *Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations*, Cambridge 2017.

Shakarian P., *The 2008 Russian Cyber Campaign Against Georgia*, „Military Review" 2011, November–December.

Wallace D., *Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis*, „Tallinn Paper" 2018, No. 11.

Wexler L., *International Humanitarian Law Transparency*, „Illinois Public Law Research Paper" 2013, No. 14–11.

Summary

The purpose of this study is to present the modern challenges facing the armed forces in examining the legality of means and methods of warfare, especially means and methods of warfare used in cyberspace. The study presents the method of military review in the context of Art. 36 of Additional Protocol I of 1977 and the need to extend it to modern means and methods of warfare. In addition, the positions of the states on the application of the military review to means and methods of warfare in cyberspace are presented.

Keywords: military review, international humanitarian law, armed conflict, means and methods of warfare

PRZEGLĄD UZBROJENIA W KONTEKŚCIE CYBERWOJNY. ARTYKUŁ 36 PROTOKOŁU DODATKOWEGO I Z 1977 R. W PRAKTYCE

Streszczenie

Celem niniejszego opracowania jest przedstawienie współczesnych wyzwań stojących przed siłami zbrojnymi w zakresie badania legalności uzbrojenia, w szczególności środków i metod walki używanych w cyberprzestrzeni. W artykule omówiono metodę badania legalności uzbrojenia w kontekście art. 36 Protokołu dodatkowego I z 1977 r. oraz konieczność jej rozszerzenia na nowoczesne środki i metody walki. Ponadto zaprezentowano stanowiska poszczególnych państw odnośnie do stosowania przeglądu uzbrojenia do środków i metod walki w cyberprzestrzeni.

Słowa kluczowe: przegląd uzbrojenia, międzynarodowe prawo humanitarne, konflikt zbrojny, środki i metody walki