JOURNAL OF MODERN SCIENCE

6/60/2024

www.jomswsge.com

DOI: 10.13166/jms/197017

ZBIGNIEW WITKOWSKI

Nicolaus Copernicus University
in Toruń, Poland

ORCID iD: 0000-0003-3220-2697

YOU WANT PEACE ? GET READY FOR WAR … IN CYBERSPACE

 The article is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA)

Abstract

Objectives: A phenomenon is emerging in relations between states that is the opposite of a declaration of war, i.e. the phenomenon of 'unspeakable war', which, according to US experts, may even lead to a so-called 'electronic Pearl Harbour'. This is because a cyber attack can ultimately take the form of... cyber warfare. In the past 20-25 years alone, we have been confronted with a situation we had not anticipated: that "destructive and disruptive actions are taking place above our heads", that cyber warfare is almost universal and at the same time invisible, because conventional weapons are not used.

Material and methods: The research was carried out using dogmatic-legal, historical and comparative legal methods.

Results: There seem to be sufficient reasons prompting the creation and harmonisation of national and international legal norms in the sphere of war. Remaining in international law and domestic constitutional law in the blissful conviction of the legitimacy of persisting in a sphere of terminology that excludes or weakens at least the meaningfulness of the concept of "war" and abrogating it in favour of a softer-sounding concept of, for example, a "state of defence" and in the need to emphasise one's entirely peaceful attitude in international relations, ceases to have its hitherto undisputed justification.

Conclusions: To be precise, the impact (attacks) on the adversary affects its : defence systems, infrastructure (including so-called critical infrastructure), society, key state institutions and political elites. If such targets are targeted through the Internet, computers and other means of storing and distributing information to attack the information systems of the victim state, it is reasonable to call such actions cyber warfare, or cyber warfare.

Keywords: *cyberspace, cyberwar, cyberterrorism, information technology, state of war, armed violence, armed conflict*

Introduction

Since ancient times, the leaders of many states, in order to ensure the continuation of their power, for their defence and the defence of their subjects, have built and maintained heavily armed armies. This was done in the face of the not at all theoretical only risk of the emergence of political rivals, eager to enlarge the territories of their own states and eager for warlike conquests. Today, changes have taken place and are still taking place in the space of inevitable military conflicts, which make it necessary to face not only the inadequate terminology in the constitutions concerning the aforementioned issue, but also its consequences in the real world.

Already Napoleon Bonaparte used to say that *good propaganda means more than a hundred divisions of an army*. In view of the completely new phenomena in this field, when we talk about cyber-attacks, cyberwar, infowar, netwar, information warriors, information dominance, cyberspace defence, hybrid warfare, full-scale warfare, so-called 'new low-intensity warfare', the real world, the real world, the real world, the real world. new low-intensity wars, on terrorist wars and asymmetric wars with the involvement of external actors, on information age warfare, it is worth considering their impact on peacetime reality (Sienkiewicz & Świeboda, 2009, p. 80 et seq.; Aleksandrowicz, 2016, p.10).

Some remarks on war and peace in the culture of antiquity

Perhaps the most famous statement for centuries concerning war as a negation of peace is the well-known Latin maxim *Si vis pacem, para bellum*, i.e. *If you want peace, get ready for war*. A more sophisticated translation of this phrase is *Prepare for war, if you cannot bear peace*. This sentence is a paraphrase of a phrase from the Prologue to the work 'On the Art of War' dedicated, probably to Emperor Theodosius, by Vecetius, a Roman historian from the 4th century AD. The virtues of valour, martial craftsmanship and military knowledge were usually highlighted when thoughts on war or its related consequences were uttered, although peace as a state was also usually appreciated most. It was admittedly said that *Vim vi repellere omnia iura permittant – to repel force by force, all laws permit*, it was also believed that *Pax melior est quam iustissimum bellum – peace is better than the fairest war*. This thesis was said to have been made by the historian Titus Livius – 59 BC – 17 AD. Admittedly, soldiers were inculcated with the virtue of valour and commanded their homeland to *Diligere ex toto corde, et in tota anima*, i.e. *to love it with all your heart and with all your soul* and reinforced with a vision of valour expressed in the equally widely known phrase over the centuries *Dulce et decorum est pro patria mori – it is sweet and honourable to die for the fatherland*, Pliny the Younger, a lawyer and Roman official (61-oc.113 A.D.), in his Letter to Tr*ajan*,

aptly put it when he wrote the following warning: *Bellum nec timendum, nec provocandum. – One should neither fear war nor provoke it*.

War and peace as concepts in the constitutional traditions of England and Poland

War, therefore, has always been feared as 'organised violence'(Prokop,2012,p.101) and therefore as an extremely dangerous and ultimate instrument of external policy. At the same time, it was not hesitant to provoke it in order to achieve set political goals and benefits. Over time, however, the horrors of wars made politicians themselves also understand the necessity of limiting state leaders and self-restraint in taking the ultimate means of resolving disputes naturally present in the international community by military or force. From the time of the Petition of Right (Prokop,2012,p.98) enacted in England, under Charles I, in 1628, the concepts of war and time of war entered permanently into the political language, and when the written constitution was born, these concepts also found their way into its pages. In Poland, too, the reflection on regulating the issue of declaring war and making peace has a long constitutional tradition framed even in certain patterns. These were set by the Constitution of the 3rd of May 1791 (Articles VI and VII), the Constitution of 17 March 1921, the Constitution of 23 April 1935, and even the Constitution of the People's Republic of Poland of 22 July 1952. These models oscillated from denying the executive the right to *declare war and make peace* and placing these decisions in the hands of the Chamber of Deputies, thus recognising the assumption of parliamentary prudence and emphasising its role as a collective assembly (1791), through the right to declare war and make peace placed in the hands of the President of the Republic, although this act still required the prior consent of the Sejm (art.50), thus still maintaining a thread of connection in the exercise of this power with Parliament, but this meant only a formal appreciation of it. The April Constitution of 1935 openly broke with this even symbolic appreciation of the Sejm, and placed decisions on the state of war and peace in the hands of the President of the Republic,

making this competence his personal prerogative (Art. 12(f)). This corresponded to the conviction, which often persists to this day, that *from the point of view of the need for speed*, the executive is better equipped to respond to these threats *(Wójtowicz,1997,p.124).From 1952 to 1997 the Constitution placed the decision on a state of war in the hands of the Sejm, and if the Sejm was not in session, this competence was taken over by the collegiate head of state, i.e. the Council of State. The latter solution is referred to in the current Constitution of the Republic of Poland of 2 April 1997. Article 116(2) stipulates that "the Sejm may adopt a resolution on the state of war only in the event of an armed attack on the territory of the Republic of Poland or when international agreements impose an obligation of joint defence aga*inst aggressio*n. If* the Sejm cann*ot convene, a state of war shall be declared by the President of the Republic*. In a situation where the competence of the President of the Republic here has a clearly visible substitute or reserve character (Nowak,2018,p.245), it is legitimate to state only a procedurally priority power of the Sejm. For materially speaking, despite the apparent elevation of the rank of the Sejm as an element of the structure of the legislature and the appreciation of its competence in the sphere of foreign policy, it must be acknowledged that the above specific competence of the Sejm, is *de facto of negligible importance* (Grzebyk,2010,p.441). This is especially the case when juxtaposed with the constitutionally unambiguous designation of the Council of Ministers as that very entity *which conducts the internal and foreign policy of the Republic of Poland*(cf. art.146(1) of the Constitution). Besides, there is always a greater risk of tardiness in the action of a collegial body such as the Sejm, when, meanwhile, the decision to enter a state of war must usually be taken with sufficient speed. To this end, different varieties of parliamentary governments shape different normative scenarios providing for the necessity of cooperation between the legislature and the executive in the introduction of a state of war, as well as states of emergency (Prokop,2012, p.356 and Witkowski, Szewczyk, Serowaniec,,(2018), Civilian control over the armed forces and their political neutrality as obligatory constituent factors of the democratic model of supremacy over the army, in Model of civilian and democratic control of the executive over the armed forces of the Republic of Poland,p.11-25).

Analysing the provisions of contemporary constitutions concerning possible internal and external conflicts today, the impression arises of a certain inadequacy of the terminology used therein for the real transformations that have already taken place then and are still taking place in the space of inevitable military conflicts. Indeed, we have been talking for a long time about cyber-attacks, cyber-wars, wars in cyberspace, cyber-terrorism, hybrid wars, etc. (Grzebyk, 2010,p.442 and Dobrzeniecki,2018, p.180 et seq.).This means that to the known three classical *theatres of war* until recently, i.e. land, sea and air space, a fourth *theatre* has been added, i.e. space, and now additionally a fifth *theatre*, i.e. cyberspace (Lakomy, 2015,p.9).

Against this background, the use of the terms *war*, *state of war*, *time of war* (also in the Polish constitution) must be regarded as unfortunate and even as using terminological anachronisms, as well as an action which bears witness to a failure to notice the long-standing avalanche of changes which have actually taken place, and are still taking place, in the sphere of ever-present armed conflicts (Grzebyk, 2010,p.442 and p.444). Additionally, it is worth noting that the term 'war' in international documents has been systematically replaced since the 1960s by the terms 'armed conflict' or 'armed action' (Grzebyk,2010,p.443), but even here the legal solutions remain far beyond the achievements and exponential progress of the ongoing technological revolution. It is this tremendous development of information technology that determines the constantly far-reaching qualitative changes in the security environment (Aleksandrowicz,2016,p.9). State information security is becoming a concept inextricably linked to the notion of national security. These changes provoke the emergence of a new type of threats to state security in conjunction with the existence of cyberspace, giving rise to entirely new possibilities for taking hostile or even merely harmful actions in it (Aleksandrowicz,2016,p.9).

Cyberspace as a new environment for warfare and warfare and the responses to this situation by the civilised world and NATO

Although cyberspace has become such a new environment for warfare or even war, and the new threats are so diverse and less predictable, and sometimes less visible, to describe even a very serious conflict between its parties, *a number of concepts that have long been established in science, but more recently their connotations have begun to raise questions* (Aleksandrowicz,2016,p.16) are still used. All the more so as the scale or magnitude of risks, threats, incidents indicative of gross misuse of the achievements of the cyber revolutions must be of concern. There is no doubt that information and communication technologies have clearly begun to gain political relevance and behaviours generated from them, e.g. cyber attacks, have begun to be recognised as a new, convenient (and most importantly) effective means of exerting political pressure (Lakomy,2015,p.9). The literature shows as unprecedented the cyber-attack on Estonia in April/May 2009 and the cyber-attacks during the phase of increasing tensions in relations between North Korea and South Korea in 2011 and 2013(Lakomy,2015,p.9).

In view of the fact that the relationship between advances in information and communication technologies and natural political, economic and cultural processes is rapidly growing, we are witnessing an increasing interest in these phenomena on the part of the social sciences, including the legal sciences, political sciences, military sciences (the art of war) and the science of international relations (Lakomy, 2015,p.9.).With the naked eye we can see how far and seriously ICT threats and various real incidents impinge on the sphere of national and international security. This situation triggers the emergence and perpetuation of new concepts, which have already been mentioned above and culminate, for example, in such new terms as cyber warfare and cyber terrorism. There are more such terms in their ever-proliferating net of concepts, and new ones are constantly appearing. However, the clue of the problem is not that they arise, but that even among experts there is no consensus on their understanding, because they are like the entire 'terminology of the information age…vague, ambiguous and elusive' (A thesis put forward by M. Dunn-Cavelty in 2008 and cited by

Lakomy, 2015,p.10). It appears that this fifth theatre of war, i.e. cyberspace, is folding in such changes in politico-military conditions and generating such advances in the wide and such a range of new means of warfare in the catalogue of modern warfare that numerous concepts hitherto well-established in science are beginning to raise questions. This makes it urgently necessary to revise them by reviewing their meaning. For some concepts are changing their meaning or even mark the birth of new phenomena. Such key concepts as war, armed conflict, conflict between states, armed violence, organisation or armed forces have been pointed out (Balcerowicz, 2013,p.85 et seq.). Such concepts, including the notion of war, armed conflict and the use of force, are constantly disputed in the science of public international law. Even though concepts such as aggression, force, self-defence, armed aggression, intervention are known to the Charter of the United Nations, they are nowhere given a definition (Grzebyk,2010,p.45 et seq.). It seems that also the science of constitutional law may have significant problems here, because here, thanks to the use of the latest means of information technology in the course of war, the goal of war, which is after all to impose one's will on the opponent by depriving him of the ability to fight, can be achieved without a single shot. Indeed, it is reasonable to argue that, after all, 'the nature of war is changeable, only its essence remains unchanged' (Aleksandrowicz,2016,p.17). How, in the conditions of actions using means of information technology, to assess with certainty the existence of the prerequisites for the duration of a state of war or armed attack from Article 5 of the NATO Treaty and to distinguish, for example, from the so-called spontaneous war in cyberspace, i.e. without the use of classical armed violence ? (Aleksandrowicz,2016,p.22).

NATO leaders in 2014, at the organisation's Summit in Wales, recognised that Article 5 of the Washington Treaty could also apply in the event of a major cyber attack on one of the allied states, followed by the NATO Summit in Warsaw in 2016. NATO recognised cyberspace as a new domain of warfare.

The same is true in our legal state of affairs with the term 'time of war' in Article 134(4) of the 1997 Constitution of the Republic of Poland. It is, moreover, used by 40 laws and 70 executive regulations despite the fact that the term has not been normatively defined and gives rise to differences in interpretation (Surmanski,2014,p.95 et seq.).

While spaces such as land, sea and air have been and continue to be spaces 'mastered' by man, cyberspace as a new combat environment has been 'created' by man (Aleksandrowicz,2016,p.23) and is so radically different from the aforementioned that it requires an entirely new doctrinal, normative and jurisprudential reflection. This applies to many disciplines of law including, in particular, international, constitutional and criminal law. This is because there is a lack of elementary legal norms relating to the environment in which the struggle is conducted, the methods and means permitted and prohibited. As long as doctrine and jurisprudence do not fill these existing deficiencies and gaps we will be dealing with a real and deep legal vacuum (Aleksandrowicz,2016,v.23). Such attempts are being made in NATO, among others, and the aftermath is the expert report of its Cyber Defence Center of Excellence entitled. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (This document having as its basis the Russian hacking attack on Estonia in 2007 is discussed by Aleksandovich, 2016,p.24 and Malycha, 2016, p.214.) It considered, inter alia, the Estonian *casus* and the case of Russia's 2008 cyber attacks against Georgia *in* terms of the existence in both cases of the so-called *ius in bello*, i.e. the existence or non-existence of the *sine qua non* prerequisite of the existence of a real armed conflict (Aleksandrowicz,2016,p.24). In the absence of progress in sorting out the legal fields on the issues at stake and retaliatory actions being taken by the attacked party, there is a real risk of the attacked states undertaking desperate and at the same time gambling interpretations or reinterpretations of existing norms according to the risky principle of "necessity knows no law", which inherently degrades the meaning and significance of law, undermining its role as an important regulator of social relations in every dimension (Aleksandrowicz,2016,p.25 and 27-28). This, in turn, implies a great risk of placing oneself in the role of a violator of international law despite the fact that one was effectively the attacked party, because an autonomous military response to a spontaneous cyber-attack based on Article 51 of the UN Charter could be considered an abuse of the right to self-defence, unless the attack was directed at the command and communication systems of the armed forces, then a cyber-attack could be considered a prelude to a classic military attack and then pre-emptive military action would be justified (Aleksandrowicz,2016,p.26). However, here too, care would have to be taken to respect the principle of proportionality of the retaliation measure used.

Risks of harmful use of cyberspace and so-called unspeakable war

So we already know that modern cybertechnologies can serve the good of mankind, but their rapid development in the 20th and 21st centuries has shown that they can be dangerous and that they can also serve the harmful use of cyberspace. They can even become deadly weapons of war on our planet. This is why they have sometimes coined the worrying name of *D-weapons*, i.e. Digital Weapons (= digital weapons) (Malycha,2016,p.204), which most of the world's states already have access to today, but worst of all, various non-state actors also have wide access to them. By this we mean *terrorist groups, companies, political or ideological extremist groups, hackers and international criminal organisations*(Malycha,2016,p.204 and the lietartura,p.210-211 cited therein (especially fn.24 – p.211). It is obvious, unfortunately already verified in the modern world, that no matter who possesses such weapons, their use *without a single gunshot can paralyse institutions and even states, can overthrow governments or ruin banks, and push ordinary citizens to take their own lives* Malycha,2016,p.204). In a situation where electronic equipment is used by the army, police, special forces, health services and numerous institutions with a statutory duty to protect citizens, in the event of a cyber-attack, depending on its purpose, sensitive citizen (private) data such as payment card PIN numbers, social security numbers, bank account numbers remain at risk and there is a huge risk of revealing private preferences, interests and the risk of identity theft(Malycha,2016,p.203).

The state-to-state relationship gives rise to a phenomenon opposite to the act of declaring war, i.e. the phenomenon of 'unspeakable war', which may even lead, as experts in the USA say, to a so-called 'electronic Pearl Harbour'(Aleksandrowicz, 2016,p.13), or an 'electronic Waterloo'(Lakomy,2015,p.8). This is because a cyber-attack in an extreme situation can ultimately take the form of… cyber-war. We have come, in the last 20-25 years alone, to a situation where we remain completely unaware that *destructive and destructive actions are taking place above our heads* (Malycha, 2016,p.223), that cyber warfare is almost universal and at the same time invisible, because conventional weapons are not used in it. In reality, however, the targets of attacks are installations that ensure

the security of the state, i.e. communication systems at the central level of the state, reconnaissance and command systems of the Armed Forces, targets that ensure the maintenance of energy production, water supply systems, gas supply systems and, finally, systems that serve to ensure the military security of the country. In shorter words, the impact (attacks) on the adversary affects its : defence systems, infrastructure (including the so-called critical infrastructure), society, basic institutions of the state and political elites (Malycha,2016,p.221). If such targets become the object of an attack carried out through the Internet, computers and other means of storing and distributing information to attack the information systems of the state of the victim of the attack, it is justified to call such actions cyber warfare, or cyber warfare.

And these are the reasons prompting the creation and harmonisation of national and international norms in the sphere of war. Remaining in international law and domestic constitutional law in the blissful conviction of the legitimacy of persisting in a sphere of terminology that excludes or weakens at least the meaningfulness of the concept of *war* and abrogating it in favour of a softer-sounding concept of, for example, a *state of defence* and in the need to emphasise one's entirely peaceful attitude in international relations, ceases to have its hitherto undisputed justification.

Cyberspace as a new dimension of foreign policy

It cannot be overlooked that the importance of cyberspace in international relations has increased in recent decades to such an extent that it is reasonable to argue that cyberspace appears to us as a new dimension of foreign policy (Lakomy,2015,p.10). Cyber-attacks in it are sometimes undertaken to pursue states' own objectives in the international space, which in turn activates and broadens situations of state rivalry in the ICT space. The attractiveness of cyberspace is enhanced by, among other things, its unimaginable openness and at the same time complex architecture, unimaginable potential and lack of established legal and political rules. (Lakomy,2015,p.10). In addition, its attractive features such as aterritoriality, supra-statehood, speed of transformation, and innovation are mentioned (Worona,2017,p.23-24) which

makes it so that the *information and telecommunication technologies used in it can pave the way for the growth of non-state political structures, further devoid of the burden of bureaucratic hierachy*(Worona,2017,p.23-24 and Lakomy, 2015,p.10-11). This makes *cyberspace lack a unified character.(…) on the Internet there is no central data storage, control point or single communication channel. It is not possible, from the point of view of the state of the art, for a single entity to control all the information transmitted over the Web. As a result, the Internet is the first ever significant global institution that does not have a single decision-making centre* (Worona, 2017,p.25. This statement is cited after its author – Dobrzeniecki, 2004, p.25).

Such a situation has made it possible to see the primacy of states' rivalry in cyberspace over conciliatory aspirations and willingness to undertake cooperation in the current century (Lakomy,2015,p.11).The forms of this rivalry are many and varied. These include hacking, hacktivism, patriotic hacktivism, cyber espionage, cyber terrorism and finally armed operations in cyberspace (Lakomy,2015,p.19). Documented examples in this regard are, with security and foreign policy implications, cyber interventions in the relations of Russia with Estonia, Russia with Lithuania, Russia with Georgia, Israel with Syria, Israel-USA with Iran, US with China and North Korea with South Korea (Lakomy 2015,p.20).

All this is causing many countries and international organisations (e.g. North Atlantic Alliance, European Union) to adopt their military and cyber security strategies, build and invest in ultra-modern research centres. In 2009, the US established the Military Cyber Command, subordinate to the US Army Strategic Command, responsible for the operation of Department of Defence information networks and planning military cyber operations (Malycha,2016,p.221 including fn.48). Cyber commands exist in NATO (NATO Cooperative Cyber Defence Centre of Excellence) and from 2019 in the Polish Armed Forces. In Poland, these are the Cyber Defence Forces under the Cyber Defence Forces Component Command.

The experience of Russian cyber-attacks on Estonia, Georgia and Kyrgyzstan has led the Americans, in a document outlining their World War III war plans for 2020-2040, to predict that 'it can be assumed that the next wars will begin with the creation of artificial information chaos, followed by a coordinated hacking attack and control of cyberspace' (Malycha,2016,p.222). This control of cyberspace will cause the attacker to gain the upper hand and build a convenient

focus by tipping the balance of the attack at a convenient time and place. Experts estimate that *broadly incapacitating or paralysing the communication and navigation system and with the attack victim's logistical system already destroyed or 'deceived', executing devastating conventional strikes against such a disorganised victim's system will only become a matter of time* (Malycha,2016,p.223).

In this situation, there is no doubt that cyber wars are changing the geopolitical order of the modern world. Cyber wars mean that the threshold of war has unfortunately been brutally crossed. Characteristically, at the apogee of the massive Russian cyber attack on Estonia in 2007, the attack so degraded the structures of the state that the Israeli security expert G.Evron, who was in Estonia at the time, stated that *with this Russian cyber bomb, Estonia was almost pushed back to the stone age* (quoted by Malycha,2016,p.215).

Paradoxically, the new threats to the national security of states brought about by the IT revolution, and despite the fact that effective cooperation mechanisms against such threats are still lacking, mean that this desirable scope for state cooperation in cyberspace is steadily growing. This means that cyberspace has its unquestionable potential and represents a new dimension in the field of state cooperation capable of countering its harmful use.

Conclusion

In the meantime, however, we must acknowledge as absolutely accurate the theses expressed on 28 February 2024 in a speech by EC President Ursula von der Leyen to the plenary of the European Parliament, who stated : In recent years, many European illusions have been dispelled. The illusion that peace is sustainable. (…) When we look around us, it becomes clear that there is no longer any room for illusions. Putin has used the peace dividend to prepare for this war. As a result, the world is as dangerous as it has not been for generations" (Palasinski,2024, p.4).

During the Congress of the European People's Party in Bucharest on 6 March 2024, also Polish Prime Minister D.Tusk stated with concern: *The times of peace and quiet are gone, the post-war era has passed. We are living in the pre-war era, for some of our brothers it is not really even pre-war anymore, but it is war, full-scale war in its cruellest form*(Youtube, 2024).

References

Aleksandrowicz, T.R. (2016). *Agresja w cyberprzestrzeni. Problematyka art.51 Karty Narodów Zjednoczonych. Uwagi de lege lata i de lege ferenda, w: Współczesne problemy prawa*, t.2 *Nadużycia prawa*.(red. Nowicka I..Mocarska D.). Szczytno.

Balcerowicz, B. (2013). *O wojnie, o pokoju. Między esejem a traktatem*, Warszawa.

Dobrzeniecki, K. (2004). *Prawo a etos cyberprzestrzeni*, Toruń.

Dobrzeniecki, K. (2018). *Prawo wobec sytuacji nadzwyczajnej. Między legalizmem a koniecznością*,Toruń.

Grzebyk, P. (2010). *Odpowiedzialność karna za zbrodnię agresji*, Warszawa.

Lakomy, M. (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice. –

Małycha, J. (2016). Cyberwojna, 4/20, Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia, Ak ademia Sztuki Wojennej.

Nowak, K. (2018). *Kompetencje głowy państwa w zakresie zwierzchnictwa nad siłami zbrojnymi i bezpieczeństwa państwa w polskim prawie konstytucyjnym*, Rzeszów.

Pałasiński, J. (2024). https://www.facebook.com/iacek.palasinski, s.4/22 (dostęp 07.03.2024).

Prokop, K. (2012).*Modele stanu nadzwyczajnego*, Białystok.

Sienkiewicz, P.. Świeboda, H. (2009). *Sieci teleinformatyczne jako instrument państwa – zjawisko walki teleinformacyjnej*, w: M.Madej, M.Terlikowski (red.) *Bezpieczeństwo teleinformatyczne państwa*, Warszawa.

Surmański, M. (2014). *Pojęcie czasu wojny oraz problemy wynikające z jego niedookreśloności w polskim systemie prawnym, Bezpieczeństwo Narodowe*nr II/30, Warszawa.

Witkowski, Z., Szewczyk, M., Serowaniec, M. (2018). Cywilna kontrola nad siłami zbrojnymi i ich neutralność polityczna jako obowiązkowe czynniki składowe demokratycznego modelu zwierzchnictwa nad armią, (w:) Model cywilnej i demokratycznej kontroli egzekutywy nad siłami zbrojnymi Rzeczypospolitej Polskiej. Toruń.

Wójtowicz, K. (1997). *Prezydenckie uprawnienia nadzwyczajne (analiza prawnoporównawcza)*.w: *Ustrój i struktura aparatu państwowego i samorządu terytorialnego*, red. W.Skrzydło, Warszawa.

Worona, J. (2017). *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy, (doktorat)*. Białystok.

Youtube.com/watch?v=faMBi8x57PA (dostęp 08.03.2024).