# CYBER SECURITY AND THE INTERNATIONAL LAW

***Peter Vršanský, Daniel Bednár***
*Comenius University in Bratislava, Faculty of Law*

**Abstract:** The Cyber security topic becomes a complex, interdisciplinary and multidimensional problem in the contemporary theory and practice of the International Law.

**Key words:** Cyber security, International Law, Cyber Attacks, Regulation

***Motto:***

*The sovereign States apply their national law within their territories and their national interests outside their territories.*

## 1 INTRODUCTION

The Cyber security is a complex, interdisciplinary and multi-dimensional problem.

The complexity of the issue consists in a variety of the challenges that have emerged with respect to the Cyber security issue in international relations. However, many crucial actors, who are involved in the multiply Cyber security activities, are not the sovereign States at the time being. The Non-governmental bodies, the supra-national private corporations, various natural and legal persons and other legal subjects of law actively engage in the Cyber security related matters in our days. Ultimately, the autonomous self-executing IT systems *à la* "Matrix", which have emancipated themselves from the Humankind's control, might commence to launch "their-own-way" acting in the Cyber security area one day.

The Cyber security topic is an interdisciplinary problem. The Public International Law norms, the Private International Law norms, the Interntional commercial law norms, the EU law regulations as well as the domestic law norms, included the constitutional law norms, civil law norms, commercial law norms, criminal law norms, administrative law norms and other law norms govern the Cyber security issue at the time being. Furthermore, the Cyber security related issues do not refer only to material law circumstances, to processual law norms but also to conflicts of laws as well. Regardless of this, still one cannot use the argument *a completudine* with respect to the existing Cyber security law regulation. The existing law regulations do not cover all particular aspects of the problem. Majority of the Cyber security issues are not yet covered by "hard law" or even "soft law" norms. The process of codification and/or progressive development of the normative regulation in this field are not in capacity to respond, in an effective way, to variety of the rapidly emerging problems that have originated both from the past needs and future challenges.

The Cyber security issue is a multi-dimensional problem to the effect that it comprises, besides the various legal aspects, a bulk of miscellaneous political, security, economic, legal, social, technological, psychological and cultural aspects. They all have strong impact on the evolution of the general and particular problems, which occur within the Cyber security area.

Thus, the international community as a whole, the individual States, the relevant international and regional organizations, they all should devote their attention and energy to further vigilant analysis of the Cyber security issue on the international, regional and national levels.

The Cyber security issue becomes the priority to the effect that it has been inflicting many areas of the sovereign States activities. The magnitude of peril that emerges from the Cybercrime attendant circumstances is unpredictable. Likewise, the amount of conceivable damages that relate to the Cybercrime is unanticipated at the time being. Nevertheless, the Cybercrime cases that have yet occurred in the international relations clearly point out the threat. The Cybercrime puts at risk the global peace and security, the peaceful development of the international relations on the daily basis.

## 2 METHODS OF ANALYSIS

In our view, only a profound historic, systemic, semantic, grammatical, logical and legal analysis of the Cyber security related matters would provide the international community of States with the due answers and pragmatic solutions how to effectively deal with the challenges that have been rapidly emerging.

### Historical analysis

The historic analysis of the problem will help the international community of States to understand better the evolution of the Cyber security issue in its historic perspective. As far as analysis of the legal texts is concerned, the historic analysis will help us to learn more about the partial phases of the "legal life" of the relevant legal documents. It seems to be very important to take into account the specific time limits, in which the sovereign States adopted the texts of the respective legal documents, when they made reservations and objections to reservations with regard the texts. It is necessary to know, when the relevant legal texts have entered into force, when the amendments and modifications of the text entered into force, and last but not least, when the decisions on termination of the respective texts entered into force.

### Systemic analysis

The systemic analysis of the Cyber security issue would provide the international community of States with a due information concerning the Cyber security issue's location within the International Law system, within the regional law systems and within the domestic law systems. The systemic analysis shows us the contextual position of the particular Cyber security issues within the structure of the individual legal documents (preamble, operative text, transitive provisions, annexes, and so on) as well. Moreover, the systemic analysis provides us with information on a broader contextual linking of the Cyber security issue to other relevant aspects of the problem under consideration. For example, on the agreements or unilateral acts adopted in the process of preparation of the relevant legal documents. Likewise, on the subsequent agreements, unilateral acts, subsequent practice or other relevant rules of the International Law, concerning the application and interpretation of the respective legal documents.

## Semantic and grammatical analysis

The semantic and grammatical analysis would provide the international community of States with a correct definition of the "traditional meaning" of the basic Cyber security issue terms that should be correctly used in the relevant legal texts in the light of their objects and purposes. Despite of the fact that many writers devote their attention to the Cyber security related matters trying to formulate the respective definitions, there does not exist a generally accepted clear-cut written definition of the term "Cyber security" in the contemporary International Law.

Some authors share the view that the "Security is a process not an end state", the "Security is the process of maintaining an acceptable level of perceived risk" and/or the "Security has three main features", *i.e.* – integrity, availability and confidentiality. [1] The UK Cyber Security Strategy, 2011 defines the Cyberspace as follows: "Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services."[2]

Bearing in the mind the argument *a coherentia* together with the argument *a completudine*, the above approach would help the international community of States to both unify and clarify the existing terminology as well as to prevent emergence of the disputes concerning the application or interpretation of the relevant legal texts in force.

The Good Faith *(Bona Fide)* principle should govern the overall creation, application and interpretation of the existing rules. The same applies for the States aimed at the progressive development and codification of the International Law norms concerning the Cyber security topic.

Nevertheless, a serious question arises, whether and to what extent the sovereign States and the other actors wish to adopt any more detailed definition of the "traditional meaning" of the cardinal Cyber security terms in written? It seems that some actors would rather prefer adopting a "special meaning" of the terms, which would be agreed upon only on a national or regional level at the time being. Not on the International Law level. The adoption of the written universally binding "hard law" norms of the International Law, which might even possess the normative quality of *iuris cogentis*, does not seem to be very realistic at the time being.

The reason for a circumspect attitude of the sovereign States in this respect lies in the realities of the contemporary international relations, *e.g.* in the above-mentioned politic, security, military, economic, social or cultural factors that influence the behaviour of the States or other actors in the domain of the Cyber security related issues.

For example, a "special meaning" of the term "espionage" might assist to solving the discrepancy between the urgent need to fight over the terrorism and the constant obligation to protect the rights of individuals. This would also assist to preventing the problems concerning the State responsibility with respect to violation of human rights and fundamental freedoms, *e. g* violating the right of an individual to private and family life in result of the State activities aimed at fighting over the Cybercrime.

Thus, the progressive interpretation of the existing rules of the International Law would assist to regulate the urgent challenges that emerge in the transitory absence of the relevant legal regulation in the field of the Cyber security related issues.

---

[1] https://www.itu.int/en/ITUD/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf

[2] https://www.cyberessentials.org/system/resources/W1siZiIsIjIwMTQvMDYvMDQvMTdfNDdfMTdfNjMwXzEwX3N0ZXBzX3RvX2N5YmVyX3NlY3VyaXR5LnBkZiJdXQ/10-steps-to-cyber-security.pdf

There exist general, supplementary and linguistic arguments of interpretation of the legal texts that promote the general call for a more progressive interpretation of the legal texts concerning the Cyber security issues.

As provided in the articles 31 – 33 of the Vienna Convention on the law of treaties[3], these arguments of interpretation are as follows:

The Article 31 (General rule of interpretation) provides that

"1. A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."

The Article 31 paragraphs 2 and 3 contain the interpretation of the term "context" and "broader context" providing that "2. The context for the purpose of the interpretation of a treaty shall comprise, in addition to the text, including its preamble and annexes: (a) Any agreement relating to the treaty which was made between all the parties in connexion with the conclusion of the treaty; (b) Any instrument which was made by one or more parties in connexion with the conclusion of the treaty and accepted by the other parties as an instrument related to the treaty. 3. There shall be taken into account, together with the context: (a) Any subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions; (b) Any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation; (c) Any relevant rules of International Law applicable in the relations between the parties.

The Article 31 paragraph 4 stipulates that "4. A special meaning shall be given to a term if it is established that the parties so intended."[4]

The Article 32 (Supplementary means of interpretation) provides that: "Recourse may be had to supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion, in order to confirm the meaning resulting from the application of article 31, or to determine the meaning when the interpretation according to article 31: (a) Leaves the meaning ambiguous or obscure; or (b) Leads to a result which is manifestly absurd or unreasonable."[5]

In this respect, the other arguments of the legal interpretation, i. e. argument a coherentia, argument a completudine, argument a contrario, argument a fortiori, argument a simili/per analogiam, argument ab exemplo, the historic argument, the psychological argument, the economic argument, the systemic argument, the logic argument, the apagogic (reductio ad absurdum) argument, the naturalistic argument and other relevant arguments, may serve in capacity of an efficient supplementary means of the legal interpretation of the relevant texts and documents concerning the Cyber security issue regulation as well.

The Article 33 regulates the interpretation of the texts of treaties that are authenticated in two or more languages. The Article 33 stipulates, that "1. When a treaty has been authenticated in two or more languages, the text is equally authoritative in each language, unless the treaty provides or the parties agree that, in case of divergence, a particular text shall prevail. 2. A version of the treaty in a language other than one of those in which the text was authenticated shall be considered an authentic text only if the treaty so provides or the parties so agree. 3. The terms of the treaty are presumed to have the same meaning in each authentic text. 4. Except where a particular text prevails in accordance with paragraph 1, when a comparison of the authentic texts discloses a difference of

[3] https://treaties.un.org/doc/publication/unts/volume%201155/volume-1155-i-18232-english.pdf

[4] Vienna Convention on the law of treaties, Article 31.

[5] Vienna Convention on the law of treaties, Article 32.

meaning which the application of articles 31 and 32 does not remove, the meaning which best reconciles the texts, having regard to the object and purpose of the treaty, shall be adopted."[6]

## Logic analysis

The logic analysis of the relevant documents is also very important to the effect, that it uncovers the intrinsic imperfections of the relevant texts under consideration.

## Legal analysis

As far as the further legal analysis of the Cyber security issue is concerned, some more detailed answering the following legal questions seems to be very important:

1. Who are the contemporary actors in the field of the Cyber security (natural persons, legal persons, autonomous self-executing IT systems)?
2. What contemporary legal rules and norms govern the Cyber security issue (hard law, soft law, treaties, customary International Law)?
3. What is the current situation with regard to the progressive development and codification of the Cyber security issue law?
4. What peaceful means of settlement of disputes seem to be optimal with respect to solving the Cyber security challenges (International, regional, national; Negotiations, good services, enquiry, mediation, conciliation, arbitration, judicial settlement, regional agencies or arrangements, other peaceful means?)
5. What coercion means and sanctions seem to be optimal with respect to Cyber security issue?
6. How to deal with the responsibility and liability issues related to Cyber security topic? Are the circumstances precluding the wrongfulness of conduct of a sovereign State applicable with respect to Cyber security activities? How to deal with the responsibility and liability of Non-governmental or supra-national actors? Who will bear the responsibility for unlawful acting of autonomous self-executing IT systems, which have liberated themselves from any human beings control?
7. What sanctions would be optimal with regard to punishing the perpetrators of the crimes related to Cyber security issues?

The national and international institutions or Non-governmental organizations, legal experts, who are involved in research and practice of the International Law, they all have perceived many other important particular legal challenges that would deserve due attention both in the theory and practice of the International Law.[7] The United Nations Interregional Crime and Justice Research Institute (UNICRI) database contains a very interesting bibliography in this respect too.[8]

---

6 Vienna Convention on the law of treaties, Article 33.

7 See e.g. An Assessment of International Legal Issues In Information Operations, May 1999 – http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf

8 See e.g. The United Nations Interregional Crime and Justice Research Institute http://www.unicri.it/services/library_documentation/bibliographies/cyber_threats/cyber_threats_database.php

## The available International Law regulations reached their operational limits

The contemporary International Law starts to be obsolete in many fields of regulation because the adoption of new written International Law norms has delayed. On the other hand, a stagnation in the field of codification of the International Law might be interpreted as the very fact that the codification process has reached the limits that are generally acceptable by the sovereign States, as far as the written form of obligations is concerned. By and large, no relevant customary International Law norms did not come to the existence due to lack of *usus longaevus* and *opinio iuris* elements.

This applies also for creation of new principles of International Law "recognized by civilised nations", the subsidiary means like the judicial decisions, or well, the works of the well-known writers.

## The interpretative activities of "glossarists" and "post-glossarists" are inevitable

Paradoxically, even the Ex *aequo et bono* principle seems to be more practical way how to seek for mutually acceptable solutions in the field of the Cyber security related issues than exploring the "classical" obsolete sources of the written International Law in our days. Somehow, the era of the medieval "glossarists" and "post-glossarists", who had commented on the Roman Empire Law, after the former Roman Empire had disintegrated, in the transitory absence of the law norms of the newly emerging feudal legal system, is recurring in the 21th century. The contemporary "glossarists" and "post-glossarists" are commenting on the norms of the old International Law system of the Bipolar World, which ceased to exist after disintegration *(dismembratio)* of the former Soviet Union Empire, in the transitory absence of the law norms of the newly emerging International Law system of the 21th century.

## The "era of implementing the exemptions from the International Law rules" is about to displace the "era of implementing the International Law rules

The time has come to remove from the "era of implementing the International Law rules" to "era of implementing the exemptions from the International Law rules" These exemptions form a constituent part of the articles regulating the protection of human rights or fundamental freedoms end they are enlisted in various multilateral International Law instruments. The reason for such transfer in conduct of the sovereign States is the on-going process of stagnation and fragmentation of the codification process concerning the domain of the Cyber security law.

Accordingly, one should give the due attention to potential utilizing the reasonable legal, legitimate and proportionally acceptable exemptions that would allow the sovereign States to neglect, if necessary, the existing human rights and fundamental freedoms in force in cases of alleged perpetration of the Cybercrimes or in cases of taking preventive actions aimed at fighting over the Cybercrime.

For example, The European Convention on Human Rights[9] contains a variety of reasons where a member State of the Council of Europe has the right to interfere into the process of enjoyment, by the individuals, of the human rights and fundamental freedoms. The limited text of the article allows us to mention only several of them.

[9] See: http://www.echr.coe.int/Documents/Convention_ENG.pdf

As far as the *Right to respect for private and family life* is concerned, the Article 8 paragraph 2 of the Convention stipulates that "2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[10]

As far as the *Right of expression* is concerned, the Article 10 paragraph 2 of the Convention provides that "2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."[11]

As far as the right to *Derogation in time of emergency* is concerned, the Article 15 paragraph 1 of the Convention provides that "1. In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law."[12]

As far as the *Restrictions on political activity of aliens* are concerned, the Article 16 of the Convention provides that "Nothing in Articles 10, 11 and 14 shall be regarded as preventing the High Contracting Parties from imposing restrictions on the political activity of aliens."[13]

## Rebirth of the Article 107 of the UN Charter?

A progressive interpretation of the Article 107 of the UN Charter, which deals with the coercive measures adopted with regard the "enemy states" in the World War I, is another theoretical possibility how to solve a discrepancy between the urgent need to fight over terrorism within the Cyber security space on one hand ant to protect the human rights and fundamental freedoms on the other hand. The Article 107 provides that "Nothing in the present Charter shall invalidate or preclude action, in relation to any state which during the Second World War has been an enemy of any signatory to the present Charter, taken or authorized as a result of that war by the Governments having responsibility for such action."[14]

## Circumstances precluding the wrongfulness of an act of the State

Another effective solution with regard to solving the Cyber security challenges, particularly the Cybercrime problem lies in the progressive interpretation of the circumstances precluding the wrongfulness of a State's conduct, by which the State violated its international obligations, *e.g.* in the domain of the human rights protection.

10 European Convention on Human Rights, Article 8.
11 European Convention on Human Rights, Article 10
12 European Convention on Human Rights, Article 15
13 European Convention on Human Rights, Article 16
14 UN Charter, Article 107 – http://www.un.org/en/sections/un-charter/chapter-xvii-0/index.html

The International Law Commission adopted the Articles on State Responsibility in 2001. They formulate several circumstances precluding the wrongfulness of an act of a sovereign State. They are as follows[15]:

- Consent (Article 20)
- Self-defence (Article 21)
- Countermeasures in respect of an internationally wrongful act (Article 22)
- Force majeure (Article 23)
- Distress (Article 24)
- Necessity (Article 25)
- Compliance with peremptory norms (Article 26)

It would be reasonable to go into the problem and scan the available justification for use of the circumstances precluding the wrongfulness of acts of States in fighting the Cybercrimes.

By the way, the sovereign States that are members of the European Union or members of the other international governmental organizations are regularly granting their official consent with respect to the preventive activities of another States or international organizations aimed at preventing the international terrorism. For example, they give their official consent (through national courts) with regard to controlling the private IT communications of citizens even in our days. This applies also with respect to self-defence activities of the sovereign States. The collective ones or well those that are taken in conformity with the Article 51 of the UN Charter. In our opinion, it is also fully reasonable for a sovereign State to react, by implementing various effective countermeasures with respect of an internationally wrongful act of another State in the Cyber security area.

### Vienna Convention on law of treaties

The Vienna Convention on law of treaties, namely the legal argument "Fundamental change of circumstances" as set in the Article 62 of the Vienna Convention on the law of treaties, offers the sovereign States another legal possibility how to solve the different contemporary challenges related to the Cyber security area.[16]

## 3 INSTEAD OF CONCLUSIONS

According to the previous analysis, one of the most recent pertracted terms is the term "cyber warfare" or "cyber attacks" [17]. Is there a need for new law or the recent international regulation is sufficient? We would like to address it in terms of three sub-questions.

First, with respect to cyber warfare, is there a gap in international law, and if so does that pose an international legal crisis?

Second, what are the challenges to interpreting existing law or developing new international law in this area?

[15] http://legal.un.org/docs/?path=./ilc/texts/instruments/english/draft_articles/9_6_2001.pdf&lang=EF

[16] Vienna Convention on the law of treaties, Article 62

[17] See also VALUCH, J. – GÁBRIŠ, T. – HAMUĽÁK, O. Cyber Attacks, Information Attacks and Postmodern Warfare. In Baltic Journal of Law & Politics, pp. 63–89.

And, third, what might the future hold with respect to international legal development and cyber warfare?

Definitions of that term vary widely, and the range of hostile activities that can be carried out over information networks is immense, ranging from malicious hacking and defacement of websites to large-scale destruction of military or civilian infrastructure that rely on those networks. By "cyber attacks", we mean efforts to alter, disrupt or destroy computer systems or networks or the information or programs on them, which is still a broad category. That breadth – encompassing activities that range in target (military versus civilian, public versus private), consequences (minor versus major, direct versus indirect), and duration (temporary versus long-term) – is part of what makes international legal interpretation or regulation in this area so difficult with respect to *ius ad bellum* and *ius in bello*. With that in mind, *is there a gap in the law, and is it a crisis?* On the one hand, this is a very new problem. The information technologies involved are new and changing constantly and rapidly, and our dependence on information technologies and their networked architecture creates new security vulnerabilities. This raises difficult questions such as when might attacks on informational infrastructure using only bits and bytes of information – electronic ones and zeros – give rise to a right of armed self-defence, or during the course of armed conflict when might such actions violate precautionary targeting requirements or constitute grossly disproportionate civilian harm? On the other hand, though, this is a very old and common legal problem. That is, it has always been possible to wage conflict using means other than kinetic violence, and there has long been much debate and disagreement about how and where to draw such lines. During the Cold War, for example, much debate centred on questions about when the use of economic power or political interference in another state's affairs violated international law or could give rise to the right of self-defence. Ancient methods of conflict like sieges and modern ones like strategic air bombardment have prompted questions about the limits on means of warfare that have indirect (or sometimes very direct) and very devastating effects on civilians. In that regard, cyber warfare emerges within a legal framework that goes back centuries, with significant refinement and codification in the 20th Century. As to *ius ad bellum*, we look primarily to the UN Charter, including Article 2(4)'s prohibition on the use or threat of force, and Article 51's recognition of self-defence rights. As to *ius in bello*, there are treaty instruments like the Hague and Geneva Conventions, though much of that regime boils down to the core principles of necessity, distinction, and proportionality. As new technologies arise, of course, they present translation challenges for these bodies of law. They always have. During the last century, such conflict methods as proxy conflicts through support for insurgencies, counter-insurgencies, and terrorism, as well as forms of economic strangulation or political subversion, raised tough questions about legal categories and boundaries. During the first Gulf War, the coalition air campaign destroyed Iraq's dual-use electrical power system, which degraded Iraq's military capacity but also resulted in widespread and long-term civilian deprivations, therefore, raising questions about targeting distinction and proportionality. In the course of Kosovo air operations, NATO forces bombed Serbian television and radio stations because these information systems were integral to Serbian war-making capacity, again raising questions about how to classify and assess legally such targeting. Cyberattacks and cyber warfare undoubtedly present new and perhaps more difficult legal translation problems. However, the point of these historical examples is to show that these challenges differ more in degree than in kind from previous legal challenges. The law may not be as clear or as effective as we would like as we try to map cyber warfare onto it, but cyber warfare is not emerging in a gaping legal hole or creating a new legal crisis. That is not to say that there are

not *new challenges to refining the law or developing new law* with respect to *ius ad bellum* and *ius in bello*[18] of cyber warfare. Some of those challenges include:

- Substantive understanding of cyberattacks and threats: some states want to preserve the flow of information, while others want to be able to disrupt and control it, and powerful states have varying views on cyber security because of differences in international political systems and relations between the public and private sector.
- Identification challenges: it may be difficult to distinguish in real-time between offensive and defensive actions, or hostile attacks versus intelligence activities in cyberspace.[19]
- Verification problems: it will be difficult to monitor, detect, and substantiate violations of norms in this area because of technical and jurisdictional limits.
- Attribution issues: thorny issues will arise as to whether and when actions by private individuals or groups in cyberspace may be attributed to a state – both as a matter of forensics in linking cyber activities to their human perpetrator and as political matter in establishing the level of state control or sponsorship.
- Secrecy: Not only will states be very reticent and guarded over their offensive and defensive actions, they will also be reluctant to disclose information about attacks they might suffer or repel, for fear of compromising intelligence capabilities or exposing vulnerabilities. An upshot of this set of challenges is that new comprehensive treaty or interpretive consensus of existing law is unlikely anytime soon in this area (at least absent a catastrophic event). We may continue to see agreement or refinement of multilateral treaties that deal with specific pieces of the cybersecurity problem, like the International Convention on Cybercrime, which requires parties to develop criminal laws against hacking and other illicit cyber activities like computer fraud. Alternatively, we may see policy agreements among small numbers or subsets of states, like a NATO strategic concept with respect to cyber defence or joint declaration among like-minded states that seek to block information activities they view as subversive. New treaties are a long way off, though, unless the states elevate form over substance, and they negotiate and adopt treaties with vague language that papers over differences and merely restates the toughest questions So, if this prognosis is correct, it leads to my third question: *what will the future look like with regard to law in this area*? In short, we are likely to see law develop not through negotiation of comprehensive treaties but through slow and uneven development of state practice. This process could be even slower and more uneven than in past eras of radical transformation in the technology and mode of conflict, though, for several reasons related to the challenges outlined above. To an even greater degree than prior forms of warfare, cyber warfare may lack clearly discernible starting points and readily observable or provable actions and counter actions. This does not mean that legal line-drawing through un Charter and IHL interpretation or new international legal agreements is impossible with respect to issues like prohibited attacks and self-defence. It does mean, however, that while information technology continues to evolve at faster and faster rates, the processes of claims and counterclaims toward a predictable, stable outcome, or the accretion of interpretive practice commanding broad consensus, will likely be slow and uncertain.

[18] See: VALUCH, J. – HAMUĽÁK, O. Cyber Operations within the Conflict in Ukraine and the Role of International Law. In SAYAPIN, S., TSYBULENKO, E. (eds.) The Use of Force against Ukraine and International Law – Jus ad bellum, jus in bello, jus post bellum.

[19] About Cyberspace see also VALUCH, J. Kybernetický priestor a medzinárodné právo In Bratislava legal forum 2016, pp. 115–124.

This legal evolution will occur less through formal negotiation, and more through posturing and policies to advance particular interpretations by states, international organizations, and other influential actors in the international system – that is, through a process of translating old law to meet new challenges, or what Michael Resiman describes as "a process of counterclaims, responses, replies, and rejoinders until stable expectations of right behaviour emerge". Examples of this that we are seeing include us declaratory policies with regard to self-defence; the drafting of the Tallinn manual on international law applicable to cyber conflict, and reactions by states to it; the London diplomatic summit on cyber security; and diplomatic discussions among China, Russia and other states about appropriate international responses to cyber threats. In sum, (1) many issues of cyber warfare are at the same time technologically unique and novel yet also legally familiar and historically recurring; (2) some particular characteristics of cyberattacks – including the low visibility of attacks and counter-actions, likely disputes about key facts, and difficulties in establishing attribution – will make it especially difficult to build legal consensus in assessing real-world scenarios; and (3) therefore, for the foreseeable future, states will have to pursue offensive and defensive strategy within existing legal frameworks regulating force, with an eye toward incremental interpretive evolution through state practice.

## Bibliography:

BEARD, J. M. Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target under International Humanitarian Law. In Vanderbilt Journal of Transnational Law, Vol. 47 (2014), pp. 67–143.

BROWN, G. – POELLET, K. The customary law of cyberspace. Strategic Studies Quarterly, 2014, Vol. 6, pp. 126–145.,

GOSNELL HANDLER, S. The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare. In Stanford Journal of International Law, Vol. 48 (2012), pp. 209–237.

KRAMER, D. F. – STARR, H. S. – WENTZ, L. – KUEHL, D.: Cyberpower and National Security. National Defense University: Potomac Books Inc., 2009.

RID, T. Cyber War Will Not Take Place. In The Journal of Strategic Studies, Vol. 35 (2012), pp. 5–32.

ROSCINI, M. Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press, 2014.

SCHMIT, M. Classification of Cyber Conflict. Journal of Conflict & Security Law, Vol. 17 (2012), pp. 245–260.

SHELDON, J., B. Cyberwarfare: The Invisible Threat. Encyclopaedia Britannica, Book of the Year 2011.

TOBANKSY, L. Basic concepts in cyber warfare. In Military and Strategic Affairs, Vol. 3 (2011);

VALUCH, J.: Kybernetický priestor a medzinárodné právo. In Bratislava legal forum 2016. Bratislava: Univerzita Komenského, Právnická fakulta, 2016, pp. 115–124, ISBN 978-80-7160-432-7.

VALUCH, J. – GÁBRIŠ, T. – HAMUĽÁK, O. Cyber Attacks, Information Attacks and Postmodern Warfare. In Baltic Journal of Law & Politics 10:1 (2018), pp. 63–89, ISSN 2029-0454.

VALUCH, J. – HAMUĽÁK, O. Cyber Operations within the Conflict in Ukraine and the Role of International Law. In SAYAPIN, S., TSYBULENKO, E. (eds.): The Use of Force against Ukraine and International Law – Jus ad bellum, jus in bello, jus post bellum. Series: International Criminal Justice Series, Vol. 18, T.M.C. Asser Press (Springer) 2018, ISBN 978-94-6265-221-7,

ZIMMERMANN, A. International Law and 'Cyber Space'. ESIL Reflections: European Society of International Law, 2014, Vol 3, Issue 1

**Contact information:**

doc. JUDr. Peter Vršanský, CSc.
peter.vrsansky@flaw.uniba.sk
Comenius University in Bratislava, Faculty of Law

JUDr. Daniel Bednár, PhD.
daniel.bednar@flaw.uniba.sk

Comenius University in Bratislava, Faculty of Law
Šafárikovo nám. č. 6
P. O. BOX 313
810 00 Bratislava
Slovak Republic