Paweł Mielniczek
Natalia A. Hapek

Can cyberspace be recognised as a fifth warfighting domain under international law?

Czy cyberprzestrzeń może być uznana za piątą domenę działań wojennych w prawie międzynarodowym?

Streszczenie: Na warszawskim szczycie NATO w 2016 r. szefowie państw i rządów krajów członkowskich Sojuszu uznali cyberprzestrzeń za „domenę operacji, w których NATO musi bronić się tak skutecznie, jak robi to w powietrzu, na lądzie i na morzu". Choć ta deklaracja polityczna na wysokim szczeblu ma duże znaczenie strukturalne i operacyjne, pozostaje pytanie o prawnomiędzynarodowy wymiar cyberprzestrzeni. Ponieważ brak jest traktatu wprost normującego jej status prawny, niniejszy artykuł ma na celu odniesienie się do pytania postanowionego w tytule: „Czy cyberprzestrzeń może być uznana za piątą domenę działań wojennych w prawie międzynarodowym?".

Analiza rozpoczyna się od zbadania ontologicznych argumentów odnoszących się do definicji cyberprzestrzeni. Następnie przedstawione zostały argumenty funkcjonalne w zakresie znaczenia cyberprzestrzeni dla operacji wojskowych. Podjęto też próbę odpowiedzi na pytanie o wpływ cech cyberprzestrzeni na zastosowanie norm prawa międzynarodowego. W każdym z podrozdziałów przedstawiono liczne argumenty podnoszone przez badaczy, analizując je przez pryzmat aktualnych ram prawnomiędzynarodowych.

Słowa kluczowe: Wojna w cyberprzestrzeni, międzynarodowe prawo humanitarne, użycie siły, prawo konfliktów zbrojnych, domena działań wojennych

Summary: At the NATO Warsaw Summit (2016), Allied Heads of State and Government recognised cyberspace as 'a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea'. Although this high-level political declaration certainly bears structural and operational significance, there is a question about the international legal dimension of cyberspace. As there is no treaty expressly regulating its legal status, this article aims to address the question posed in the title: 'Can cyberspace be recognised as a fifth warfighting domain under international law?'.

The analysis starts with examining ontological arguments as to what cyberspace is. Then, functional arguments regarding the significance of cyberspace to military operations are presented. Next, the question of how characteristics of cyberspace influence applicability of international legal norms will be answered. In each section, multiple arguments raised by scholars are outlined and analysed through the lens of current international legal framework.

Keywords: Cyber warfare, international humanitarian law, use of force, law of armed conflict, warfighting domain

Introduction

At the NATO Warsaw Summit (2016), Allied Heads of State and Government recognised cyberspace as 'a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea'.[1] Although this high-level political declaration certainly bears

[1] *Warsaw Summit Communiqué, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*, para 70, http://www.nato.int/cps/en/natohq/official_texts_133169.htm (accessed 19 April 2017). Similarly, cyber is named a fifth domain for military operations in *Defence Cyber Strategy* (The Netherlands Ministry of Defence, 2012), p. 4, as well as *Cyberspace Operations* (U.S. Armed Forces Joint Publication 3-12(R), 2013), para I-2, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (accessed 20 April 2017) and *Department of Defense Strategy for Operating in Cyberspace* (U.S. Department

structural and operational significance, there is a question about the international legal dimension of cyberspace. As there is no treaty expressly regulating its legal status, this article aims to address the question posed in the title: 'Can cyberspace be recognised as a fifth warfighting domain under international law?'.

Ontological arguments: What is cyberspace?

To answer whether certain norms of international law are applicable to cyber warfare, firstly there is a need to clarify its characteristics. According to the *Collins Dictionary*, the word 'cyber' simply 'indicates computers'.[2] In turn, '[i]n computer technology cyberspace refers to data banks and networks, considered as a place'.[3] Although there is no legal definition of cyberspace, there are some close concepts, such as 'computer system', defined in art. 1(a) of the Convention on Cybercrime (2001) as 'any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data'.[4]

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) in art. 2(c) defines 'automatic processing' as 'the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination'.[5] The European Union law defines for instance an 'Information Society service' as 'any service normally

of Defense, 2011), p. 5, http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (accessed 20 April 2017).

[2] *Collins Dictionary*, https://www.collinsdictionary.com/dictionary/english/cyber (accessed 20 April 2017).

[3] *Collins Dictionary*, https://www.collinsdictionary.com/dictionary/english/cyberspace (accessed 20 April 2017).

[4] Polish Journal of Law of 2015, pos. 728.

[5] Polish Journal of Law of 2003, No. 3, pos. 25. A similar understanding was adopted in the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. (L119/1).

provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'.[6]

But despite the paucity in treaty language, there are already too many definitions of cyberspace in non-binding sources. The NATO Cooperative Cyber Defence Centre of Excellence, for instance, provides a robust catalogue of cyber-related terms, as defined throughout different States. Only with respect to the very cyberspace, it indicates 23 different approaches.[7] To find a common ground, instead of proposing another definition, the authors would like to indicate certain characteristics of cyberspace, as identified by various scholars.

The major controversy as to ontology of cyberspace is whether it encompasses a physical sphere. There are positive and negative answers not only among scholars, but also amid States. For instance in the UK, it is common to follow the way in which novelist William Gibson is thought to have put it first. Cyberspace is understood there as 'any large collection of network-accessible computer-based data', thereby excluding a physical dimension. In Turkey, in turn, it is described as '[t]he environment which consists of information systems that span across the world including the networks that interconnect these systems'.[8] The U.S. National Military Strategy for Cyberspace Operations once defined cyberspace as a 'domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructure'.[9]

There are those who say that cyber warfare does not exist,[10] and those who say that cyberspace is a 'wholly physical construct much like any other terrain'.[11] But it is more common not to ignore the virtual

[6] Art. 1(2), Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998, O.J. (L217/21).

[7] NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/cyber-definitions.html (accessed 20 April 2017).

[8] Ibidem.

[9] *Air Force Cyber Command Strategic Vision* (2008), p. 3, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA479060 (accessed 21 April 2017).

[10] S. Liles, et al., 'Applying Traditional Military Principles to Cyber Warfare' in C. Czosseck, R. Ottis and K. Ziolkowski (eds.), *4th International Conference on Cyber Conflict. Proceedings 2012*, NATO CCD COE Publications 2012, p. 178.

[11] Ibidem, p. 172.

dimension of cyberspace. According to the U.S. Armed Forces Joint Publication on Cyberspace Operations, it is possible to describe cyberspace 'in terms of three layers: physical network, logical network, and cyber-persona. Each of these represents a level on which the cyber operations may be conducted'.[12] Consequently, '[m]uch as air operations rely on air bases or ships in the land and maritime domains, cyber operations rely on an interdependent network of IT infrastructures …, and the content that flows across and through these components'.[13]

If we distinguish three dimensions: (a) physical – real world, (b) informational – 'where and how information is collected, processed, stored, disseminated and protected', and (c) cognitive – encompassing 'the minds of those who transmit, receive, and respond to or act on information', it becomes clear that the cyber is ontologically different from other domains.[14] Its users are not virtual, contrary to their accounts and transmitted data. But if cyber encompasses physical devices and infrastructure, these belong at least to two domains: cyberspace and land, sea, air or outer space, depending on where physical objects are located. This raises a crucial question: in order to recognize a new warfighting domain, is it necessary to establish that it is completely separable from other warfighting domains? An answer to that question will be provided

[12] 'The physical network component is comprised of the hardware, systems software, and infrastructure (wired, wireless, cabled links, EMS links, satellite, and optical) that supports the network and the physical connectors (wires, cables, radio frequency, routers, switches, servers, and computers).... The logical network layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node.... The cyber-persona layer represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. The cyber-persona layer consists of the people actually on the network. Cyber-personas may relate fairly directly to an actual person or entity, incorporating some biographical or corporate data, e-mail and IP address(es), Web pages, phone numbers, etc. However, one individual may have multiple cyber-persona, which may vary in the degree to which they are factually accurate'. See *Cyberspace Operations*, U.S. Armed Forces Joint Publication 3-12(R), 2013, p. I2-I4, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (accessed 20 April 2017).

[13] Ibidem, p. I2.

[14] *Information Operations*, U.S. Armed Forces Joint Publication 3-13, 2014, p. X, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (accessed 20 April 2017).

in the next sections of the paper. At this juncture, it would be sufficient to focus on analysing how separable is cyber: what are the specifics that distinguish it from other domains.

It is difficult to assert that only one ontological category can exhaustively define cyberspace. Naming four traditional domains as 'physical' and defining cyber as a sphere of electro-magnetic processes would include also electro-magnetic weapons and other phenomena, which are not a part of the communication process. As Brett Williams writes, '[t]he key difference between cyberspace and the physical domains is that cyberspace is man-made and constantly changing'.[15] Cyber is not, or at least not only, a physical dimension and is different from real spaces. 'Its aterritorial, borderless and ubiquitous character differentiates it from the physical and bounded spaces that are subject to legal regulation'.[16] Therefore, it is necessary to analyse other aspects of how cyber differs from traditional domains.

Functional arguments: What is the significance of cyberspace to military operations?

It can be said with a level of certainty that cyber is non-natural and constantly under construction, so that its borders and limits are not measurable. But the sea also changes its area,[17] and the outer space only recently is said to be measurable.[18] Nevertheless, cyberspace has a lot of specifics different from other domains. Nazli Choucri from the Massachusetts Institute of Technology distinguished, among others, the following characteristics of cyber: a) temporality ('replaces conventional temporality with near instantaneity'), b) physicality ('transcends

[15] B. Williams, 'Cyberspace: What is it, where is it and who cares?', *Armed Forces Journal*, 13 March 2014, http://armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/ (accessed 20 April 2017).

[16] N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 2015, p. 13.

[17] R. Nuwer, 'What happens when the sea swallows a country', BBC, 17 June 2015, http://www.bbc.com/future/story/20150616-what-happens-when-the-sea-swallows-a-country (accessed 21 April 2017).

[18] Ch. Baraniuk, 'It took centuries, but now we know the size of the universe', BBC, 13 June 2016, http://www.bbc.com/earth/story/20160610-it-took-centuries-but-we-now-know-the-size-of-the-universe (accessed 21 April 2017).

constraints of geography and physical location'), c) permeation ('penetrates boundaries and jurisdictions'), d) fluidity ('sustains shifts and reconfigurations'), e) participation ('reduces barriers to activism and political expression'), f) accountability ('bypasses mechanisms of responsibility').[19]

Sean Brandes from the U.S. Navy indicated six grounds on which cyberspace domain differs from traditional domains:

The first refers to resources, whereby cyber is relatively inexpensive and 'human capital-driven', as opposed to traditional domains, 'limited to nations with significant financial resources' and with 'industrial-based assets'.

The second refers to physics. Here, the cyber is an 'artificial construct, permeable virtual boundaries' as well as 'distributed, dynamic and non-linear'. The traditional domain, in turn, 'exists naturally' and has 'discrete physical boundaries'. Both domains function as a 'multi-use environment (government, military, commercial)'.

The third ground concerns actors. In cyber, they are 'ambiguous' and vary 'from nation-states to individuals' and from 'criminal organizations to commercial entities'. In a traditional domain, the 'identity of adversary is usually known'.

The fourth ground are effects. In cyber, these are 'global in nature', 'non-kinetic or kinetic' and the 'collateral damage on 2nd/3rd order' is of 'potentially global' effects. In turn, a traditional domain, with the exception of space is 'usually regionally focused', 'usually kinetic' (electronic warfare exception) and the collateral damage is 'limited to active battlespace'.

The fifth, cyber and traditional domains differ by 'Authorities for Offensive Action'. In cyberspace, these are 'elevated' and the rules of engagement (RoE) are 'evolving'. In the traditional domain, the authorities for offensive action are 'local' and the RoE 'established'.

The sixth, when it comes to 'intelligence support', in both kinds of domains it 'requires knowledge of adversary capabilities and intent'.

[19] N. Choucri, 'Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences', MIT Political Science Department Research Paper No. 2014-29, p. 3, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2514532 (accessed 16 May 2016).

The difference is that – with respect to cyber – intelligence support is of a "compressed timeline ('net' speed)" and the 'attribution is challenging'.[20]

The above arguments show that operating within cyber indeed differs from traditional domains. Operations within cyberspace certainly require a high specialisation and cyber units are completely different from the other units of the armed forces.[21] However, **there is ambiguity as to whether its specifics are significant enough to recognise it as a warfighting domain**. Among affirmative stances, Patrick D. Allen and Dennis P. Gilbert Jr. refer to cyber as a 'sphere of interest and influence'.[22] They claim that 'control can be exercised over an opponent in or through that sphere',[23] and that '[o]btaining dominance in the Information Sphere will likely lead to continued dominance in the four physical domains'.[24] Others call cyber a 'global commons', as the contemporary State system is 'embedded nearly as much in the cyber domain as it is in the natural environment'.[25]

Individuals distinguishing cyber as a warfighting domain observe a sizeable and constantly growing scale of cyber-threats to the national security. They argue that '[a]s a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare. Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air, and space. As such, the military must be able to defend and operate within it'.[26] Admittedly, not all the constituent members of NATO have cyber warfighting capabilities,

[20] S. Brandes, 'The Newest Warfighting Domain: Cyberspace', *Synesis: A Journal of Science, Technology, Ethics, and Policy* 2013, p. 94.

[21] See also W. Gozdziewicz, "Militias, volunteer corps, levée en masse or simply civilians directly participating in hostilities? Certain views on the legal status of 'cyberwarriors' under law of armed conflict", *European Cybersecurity Journal* 2016, Vol. 2, No. 2.

[22] P. Allen, D. Gilbert, 'The Information Sphere Domain Increasing Understanding and Cooperation', p. 2, https://ccdcoe.org/sites/default/files/multimedia/pdf/09_GILBERT%20InfoSphere.pdf (accessed 21 April 2017).

[23] Ibidem, p. 8.

[24] Ibidem, p. 10.

[25] R. Bunker, C. Heal, *Fifth Dimensional Operations. Space-Time-Cyber Dimensionality in Conflict and War*, iUniverse, 2014, p. 21.

[26] W. Lynn, 'Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs* 2010, Vol. 89, No. 5, p. 101.

but there is no necessity. Likewise is the case with outer space and no one questions it as a domain.[27]

An opposite view argues that the significance of cyber warfare is limited. 'Most cyber-attacks, once discovered, are resolved and the effects (apart from leaked information) reversed within a period ranging from hours to days'.[28] Thus, perceiving cyber as a "high ground of warfare, the one domain to rule them all and in the ether bind them, …is the wrong way to view cyberspace and what militaries can do by operating 'within' it".[29] In this respect, differently from other domains, cyber warfare 'requires that the targets have made mistakes in their implementation and use of digital equipment'.[30]

Also, the cyber is and will be intrinsically used to achieve effects in other domains, such as disabling hospitals, taking control over vehicles, hacking financial systems. Control can be exercised not exactly over opponents, but over their capabilities and means of achieving goals. Although a vehicle would not function without any electronics, the software of a tank, ship or aircraft does not make the whole vehicle belong to the cyber domain.

As Wiesław Goździewicz points out, '[s]o far there has been no cyberwar per se, i.e. an armed conflict that occurred only in cyberspace or used only cyber means and methods of warfare… Nevertheless, there are several examples of conventional armed conflicts, in which cyber means and methods have been used prior to or in parallel to conventional operations. One of the examples pertains to cyber activities attributed to Russia during the 2008 conflict with Georgia (allegedly not only DDOS attacks against and defamation of Georgian governmental web sites, but also disrupting Georgian air defence systems). The other one is linked to Operation Orchard launched in 2007 by Israeli Defence Forces against an alleged Syrian nuclear installation.'[31]

---

[27] P. Allen, D. Gilbert, op. cit., p. 1-2.

[28] M. Libicki, 'Why Cyber War Will Not and Should Not Have Its Grand Strategist', *Strategic Studies Quarterly* 2014, Vol. 8, No. 1, p. 32.

[29] M. Libicki, 'Cyberspace Is Not a Warfighting Domain', *I/S: A Journal of Law and Policy for the Information Society* 2012, Vol. 8, No. 2, p. 322.

[30] M. Libicki, 'Why Cyber War Will Not and Should Not Have Its Grand Strategist', *Strategic Studies Quarterly* 2014, Vol. 8, No. 1, p. 31.

[31] W. Gozdziewicz, 'Selected Legal Aspects of Cyber Warfare', *The Magazine of the Joint Force Training Centre* 2015, No. 8, p. 24.

How could characteristics of cyberspace influence applicability of international legal norms?

As Nicholas Tsagourias and Russell Buchan noticed, '[t]he view that cyberspace is subject to law and indeed to international law is not in dispute anymore'. Nowadays, it seems clear that the 'UN Charter applies to cyberspace' and that State sovereignty applies to 'State conduct of ICT-related activities, and to jurisdiction over ICT infrastructure within a State's territory'.[32] All of the characteristics of cyber gathered in previous sections show how cyber differs from other domains. Currently, the legal debate needs to focus on arguments, which: a) reveal that norms applicable to traditional domains are not sufficient to reach legal clarity as to the acts of cyber warfare; and b) indicate criteria for determining applicability of suggested norms on cyber warfare.

Also from this perspective, there are two opposing standpoints. The first one asserts that cyberspace 'should remain an open, decentralised and participatory space, not hampered by legal regulations'.[33] Scholars supporting it argue that 'understanding cyberspace as a warfighting domain is not helpful when it comes to understanding what can and should be done to defend and attack networked systems'. It is not clear, 'what purpose is served by calling cyberspace a domain', while cyber operations have 'tenuous' relationship to cyberspace.[34]

Recognizing the domain 'shifts the focus of thought from the creation and prevention of specific effects to broader warfighting concepts, such as control, maneuver, and superiority' (defending the domain).[35] It entails expectations that the State will protect its cyberspace 'in the same way that the Army, Navy, and Air Force keep hostile forces away' from its borders.[36] 'Then, users can hide behind the fiction that they are being fully protected and can no longer be compelled to protect themselves, thereby limiting potential lawsuits arising from third-party

[32] N. Tsagourias, R. Buchan (eds.), op.cit., p. 13.
[33] Ibidem.
[34] M. Libicki, 'Cyberspace Is Not a Warfighting Domain', *I/S: A Journal of Law and Policy for the Information Society* 2012, Vol. 8, No. 2, p. 322.
[35] Ibidem, p. 328.
[36] Ibidem, p. 333.

damage. After all, no one expects private firms to mount their own anti-aircraft weapons'.[37]

The second standpoint claims that 'the complex nature of cyberspace means we can no longer afford imprecision in the law, especially when it comes to the right of self-defense'.[38] This could refer, for instance, to attacks with no physical damage, attacks from non-state actors or to pre-emptive self-defence. Proponents of this reasoning further argue that 'representing the relationships of information among actors and information systems in a manner useful to planners and decision makers will help improve the effectiveness and efficiency of operations in and through the Information Sphere'.[39] And consequently, that 'focusing and preparing enhanced capabilities in the Information Sphere will enable superior influence and control in this domain'.[40]

The law of armed conflict, similarly to other branches of international law, is applicable to cyberwarfare. For instance, cyber-defence activities could be considered 'acts of violence against the enemy', as provided for in art. 49(1) of Additional Protocol I.[41] Within cyber, it is possible not only to ensure, but also augment compliance with four fundamental principles of international humanitarian law: distinction between civilians and combatants, proportionality, humanity and military necessity. Both cyber soldiers (as long as they fall within the definition of combatants) and cyber military objects (military computers and military cyber infrastructure) can be lawful military objectives for cyber operations.[42]

---

[37] Ibidem, p. 335.

[38] N. Jupillat, 'Armed Attacks in Cyberspace: The Unseen Threat to Peace and Security that Redefines the Law of State Responsibility', *University of Detroit Mercy Law Review* 2015, Vol. 92, No. 2, p. 116.

[39] P. Allen, D. Gilbert, op.cit., p. 10.

[40] Ibidem.

[41] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. See W. Gozdziewicz, "Militias, volunteer corps, levée en masse or simply civilians directly participating in hostilities? Certain views on the legal status of 'cyberwarriors' under law of armed conflict", *European Cybersecurity Journal* 2016, Vol. 2, No. 2, p. 13-14.

[42] M. Libicki, 'Cyberspace Is Not a Warfighting Domain', *I/S: A Journal of Law and Policy for the Information Society* 2012, Vol. 8, No. 2.

If an attempt were to be made to bring these opposing standpoints closer to each other, here are two less far-reaching statements: a) cyber may at some point require separate regulation under international humanitarian law, and b) law should be technologically neutral.[43] Regarding the first statement, it seems that separate regulation of cyber warfare would not lose precision without recognising cyber as a domain. As to the second statement, technological neutrality is useful as long as it enables law to cover the broadest possible scope of cases. However, if at one point it means that the law is not clear enough to protect various legitimate interests in cyber, a need for specific regulation should prevail.

If achieving legal precision does not depend on recognising cyber as a warfighting domain, is there any point in doing so? Opponents would argue that it may prove superfluous or even blur interpretation of international law. Therefore, the authors would like to examine how the characteristics of cyberspace could influence the issue of jurisdiction. The State's title to exercise jurisdiction over cyber 'rests in its sovereignty'.[44] The actual abilities to exercise jurisdiction depend on its technological capabilities, similarly to the enforcement capabilities in other domains.

The State exercises jurisdiction mainly over actors (people) who can be found only in physical domains. It is said that the State exercises jurisdiction over cyberspace as an object, the same as over land, sea etc.[45] At the same time, 'the State can exercise its prescriptive and enforcement jurisdiction over cyberspace and over cyber activities on the basis of nationality and territoriality' as well as extraterritorially.[46] But it is not clear what constitutes an extraterritorial jurisdiction over cyber where there are no boundaries. Rather, the States tend to claim jurisdiction over certain activities done in cyber, on the grounds that they relate to natural or legal persons under their jurisdiction.[47] Thus, so far it

[43] B. Jones, 'The Online/Offline Cognitive Divide: Implications for Law', *SCRIPT-ed* 2016, Vol. 13, No. 1.

[44] See *Lotus case (France v. Turkey)*, PCIJ Judgment of 7 September 1927, Series A No. 10, p. 19.

[45] N. Tsagourias, R. Buchan (eds.), op.cit., p. 19.

[46] Ibidem.

[47] See for instance art. 3(2)(b) of the General Data Protection Regulation. See also J. Kumar, *Determining Jurisdiction in Cyberspace* (2006), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=919261 (accessed 20 May 2016).

has not been necessary to recognise cyber as a domain for the purposes of civil, commercial or data protection law. In the next section, an examination will be made as to whether that applies also to a warfighting domain.

What is a warfighting domain?

In the beginning of this paper, the following question was posed: in order to recognize a new warfighting domain, is it necessary to establish that it is completely separable from other warfighting domains? For instance, finances, law and politics constitute domains. These are also spheres with own specifics and where the coercion does occur. What is then the difference between normal and warfighting domains?

Patrick D. Allen and Dennis P. Gilbert Jr. propose six components of the definition of a domain: a) 'unique capabilities are required to operate in that domain', b) 'a domain is not fully encompassed by any other domain', c) 'a shared presence of friendly and opposing capabilities is possible in the domain', d) 'control can be exerted over the domain', e) 'a domain provides the opportunity for synergy with other domains', f) 'a domain provides the opportunity for asymmetric actions across domains'.[48] Regarding point b), the word 'fully' allows to exclude parts of the sea from the seas as a general domain. But 'fully' means that cyber may be encompassed by other domains to a large extent. In this regard, most electromagnetic devices belong to the land domain. As to point d), it is difficult to state that control can be exerted over outer space, which already is a domain.

The abovementioned authors further describe the requirements for creating a new domain: (1) 'the capability to begin to operate in that domain is developed', (2) the capabilities 'become relatively commonplace', (3) the capabilities in that sphere 'affect capabilities in that domain', (4) 'sufficient recognition of the unique and synergistic nature of capabilities', (5) 'sufficient institutional and financial support for the domain'.[49] With respect to point (1), the capabilities to operate in cyber are constantly under development. As ancient soldiers operated

[48] P. Allen, D. Gilbert, op.cit., p. 3.
[49] Ibidem, p. 5-6.

in the land domain, similarly every State with access to the Internet or mobile networks would have a capability to operate, but it does not mean it is developed. Regarding requirement (5), it is indeed true, but not yet legally precise. Nevertheless, according to the authors, cyberspace already meets all of these criteria.[50]

The above quoted scholars propose the definition of a domain as '[t]he sphere of interest and influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects'.[51] But such a definition might as well denote economy and politics. If we proceed to describe the warfighting domain by replacing the word 'activities' with 'military activities', we would be almost compelled to ask whether the activities in cyber are aimed at achieving effects in cyber, or in other domains. What is more, some activities on land (e.g. anti-aircraft defence) indicate that the desired effects are located outside the domain of the subject which undertakes such activities (army).

Therefore, we conclude that the key legal criterion for a warfighting domain is whether or not use of force can occur exclusively within that domain. If no use of force can occur without an effect in traditional domains, cyber is not a stand-alone warfighting domain. Also the International Group of Experts which recently developed the Tallinn Manual 2.0. did not adopt an understanding that cyber is a 'fifth domain' under international law. Their argument was different: it disregards 'the territorial features of cyberspace and cyber operations that implicate the principle of sovereignty. Cyber activities occur on territory and involve objects, or are conducted by persons or entities, over which States may exercise their sovereign prerogatives. In particular, the Experts noted that although cyber activities may cross multiple borders, or occur in international waters, international airspace, or outer space, all are conducted by individuals or entities subject to the jurisdiction of one or more States'. (similarly with regard to cyber infrastructure aboard sovereign immune platforms).[52]

[50] Ibidem, p. 5-6.

[51] Ibidem, p. 2.

[52] M. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, p. 12-13.

Conclusions

In order for a cyber-attack to constitute use of force, it has to have an effect within other domains (death, injury, significant material damage) but if the military names cyber-attacks as such even if they do not constitute use of force under the UN charter, it is possible to speak of cyber as a non-legal warfighting domain.[53]

It is difficult to find a criterion which convincingly separates the cyber from other spheres. Even if the use of force is done through cyber, its effects appear in other domains. The same pertains to the threat of use of force – the purpose of using such force is to attack the targets within other domains. Even if the operation aims only at completely and permanently disabling computers, the physical devices are also a part of other physical domains (that is a tangential point of cyber and other domains). Therefore, it is possible to argue that cyber is only a dimension through which the force is applied to traditional domains.

However, if cyber encompasses physical devices, using exclusively cyber means to destroy only these devices (assuming that they considered to be personal property and are not used for controlling land/sea/air/space domains), it means that an armed attack can occur within the domain of cyber, without effects in other domains.

In the future, undoubtedly there will be an increase in cases where the effects of operations in cyber are limited to cyber. That can potentially lead to future recognition that the use of force can occur, even if the projected effects of the attack are confined to cyber. As Martin Libicki noticed, 'If cyberspace is like other domains, then under current rules of engagement for kinetic combat, U.S. forces are allowed to fire back when under fire'.[54]

According to the Tallinn Manual 2.0, 'a cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful'[55].

[53] See ibidem, p. 12.

[54] M. Libicki, 'Cyberspace Is Not a Warfighting Domain', *I/S: A Journal of Law and Policy for the Information Society* 2012, Vol. 8, No. 2, p. 333.

[55] M. Schmitt (ed.), op.cit., p. 329.

This creates a dispute over whether certain cyber operations, or activities related to cyber (e.g. affording sanctuary – safe haven – to those mounting cyber operations of the requisite severity), reach the threshold of severity required to consider it to be a use of force. 'As for cyber operations that do not cause physical damage, the qualification of use of force cannot be entirely ruled out but no consensus on a possible threshold has yet emerged'[56]

So what can be done in order to address these challenges under international law? As Albert Einstein said, 'we cannot solve our problems with the same thinking we used when we created them'. So we would rather not think of circumventing constraints and the gaps within the current international legal framework by way of creative interpretation. Especially as in practice, such an interpretation would only reflect the position of one side.

If there is a legal gap, one of the solutions would be an advisory opinion of the ICJ, expressly indicating where the gaps are, so that the UN and international community are given a clear signal of a need to gather and eliminate them. No doubt there is a need to constantly update answers as to who and what can pose a threat to international peace and security, not only by threat or use of force. At the same time, the challenge is to finally adopt a universal understanding of crime of aggression, so that any activities aiming at circumventing prohibition of use of force are deemed illegal – irrespective of whether their effect amounts to an armed attack under art. 51 of the UN Charter. Political debates 'may eventually lead to common understandings about cyber ontology or use which are then normativised in the form of legal rules'.[57]

[56] N. Jupillat, op. cit., p. 118.

[57] N. Tsagourias, R. Buchan (eds.), op.cit., p. 14.