Научная статья / Research Article
https://doi.org/10.17323/jil.2025.32003

Article 51 and cyberspace: the UN Charter constraints and the expanding frontiers of self-defence against cyber operations[1]

E. Martynova

HSE University, Moscow, Russia
eamartynova@hse.ru
ORCID: 0000-0002-8995-4462

Abstract

The United Nations Charter, at its 80th anniversary, remains the cornerstone of international law governing the use of force and the maintenance of peace and security. However, the rapid development of information and communication technologies (hereafter — ICTs) in recent decades has introduced unprecedented challenges to its application, particularly in cyberspace. The ambiguity surrounding the interpretation of key UN Charter provisions — Article 2(4) on the prohibition of the use of force and Article 51 on self-defence — in the context of cyber operations has led to legal and strategic uncertainties. States increasingly engage in hostile cyber activities that blur the line between permissible acts and prohibited use of force. This raises critical questions about attribution and international responsibility, as well as escalation risks. This paper examines how the UN Charter's framework struggles to address cyber conflicts in the context of *jus ad bellum*. Apart from the applicability of Article 51 in cyber context, the paper considers extra-Charter modalities of self-defence in cyberspace, based on the international treaties within the North Atlantic Treaty Organization and the Shanghai Cooperation Organization, to explore potential legal and institutional adaptations to uphold international peace and security in the digital age.

Key words: UN Charter, use of force, cyberspace, cybersecurity, self-defence

Citation: Martynova E. Article 51 and cyberspace: the UN Charter constraints and the expanding frontiers of self-defence against cyber operations. *HSE University Journal of International Law*. 2025. Vol. 3. No. 4. P. 75–90.

Ekaterina A. Martynova — lecturer at the School of International Law, Faculty of Law, candidate of sciences in law.

[1] The article was prepared within the framework of the research project "International Law and Process in the Metamodern Era" at the Faculty of Law of the HSE University (without funding).

Статья 51 и «киберпространство»: ограничения Устава ООН и правомерность расширения границ самообороны от кибероперaций

Е. А. Мартынова

Национальный исследовательский университет
«Высшая школа экономики», Москва, Россия
eamartynova@hse.ru
ORCID: 0000-0002-8995-4462

Аннотация

Устав Организации Объединенных Наций, вступивший в силу 80 лет назад, остается краеугольным камнем международного права в вопросах применения силы и поддержания международного мира и безопасности. Однако стремительное развитие информационно-коммуникационных технологий (далее — ИКТ), наблюдавшееся в последние десятилетия, ставит трудноразрешимые вопросы о действии положений Устава в так называемом киберпространстве. Неоднозначность толкования ключевых положений Устава ООН — статьи 2(4) о запрете применения силы и статьи 51 о праве на самооборону — в контексте кибероперaций приводит к значительной правовой неопределенности. Государства все чаще прибегают к враждебным кибернетическим действиям, которые размывают грань между допустимым поведением и запрещенным применением силы, что порождает серьезные вопросы, связанные с присвоением поведения негосударственных акторов в «киберпространстве» государствам, международной ответственностью и рисками эскалации. В данной статье анализируется, как система Устава ООН адаптируется к решению задач урегулирования киберконфликтов в контексте *jus ad bellum*. Помимо исследования применимости статьи 51 Устава ООН в киберконтексте, в статье рассматриваются формы самообороны в «киберпространстве» вне Устава ООН, основанные на международных договорах в рамках НАТО и Шанхайской организации сотрудничества, с целью выявления потенциальных правовых и институциональных механизмов поддержания международного мира и безопасности в цифровую эпоху.

Ключевые слова: Устав ООН, применение силы, киберпространство, кибербезопасность, самооборона

Для цитирования: Мартынова Е. А. Статья 51 и «киберпространство»: ограничения Устава ООН и правомерность расширения границ самообороны от кибероперaций. *Журнал ВШЭ по международному праву / HSE University Journal of International Law*. 2025. Том 3. № 4. С. 75–90.

Екатерина Александровна Мартынова — преподаватель Департамента международного права факультета права, кандидат юридических наук.

Introduction

There are scant international legally binding regulations specifically governing activities in cyberspace. The existing regulations primarily focus on cybercrime (the Budapest Convention on Cybercrime of 2001[2] and UN Convention against cybercrime adopted by United Nations General Assembly on 24 December 2024[3]) and are fairly limited in scope. The secretive nature of most national cyber policies makes it challenging to establish a widely accepted *opinio juris*, thereby complicating the development of customary law in this domain. Nonetheless, the absence of comprehensive international cyber treaties does not imply that cyber domain represents the 'wild, wild West' as famously referred to by then US President Barack Obama in 2015.[4] While many nations have chosen the 'wait and see' approach with respect to certain aspects of the international law application in cyberspace (Jiang, 2021, p. 257), others are actively engaged in the process of interpreting existing international law to meet the new challenges of the digital age. One of the key aspects of the ongoing discussion is the applicability of the UN Charter's framework on the prohibition of the use of force (Article 2(4)) and the right to self-defence (Article 51), designed for traditional armed conflict, to cyber operations. The spectrum of possible approaches ranges from the position that these provisions of the UN Charter are *sufficiently adaptable* to cyberspace, to the view that the unique nature of cyber threats — such as ambiguity in attribution, thresholds of harm, and non-State actor involvement — necessitates a *reinterpretation* or even *reformulation* of these rules.

International law governing the use of force (*jus ad bellum*) operates on a two-threshold framework set out in the UN Charter, distinguishing between 'use of force' (prohibited by Article 2(4)) and 'armed attack'[5] (which triggers the right to self-defence under Article 51). This distinction was reinforced by the International Court of Justice's 'scale and effects' doctrine in the *Nicaragua* case.[6] However, applying these concepts to cyberspace is profoundly challenging because the Charter lacks definitions for 'force' or 'armed attack' in this context. Moreover, the *travaux préparatoires* of Article 51 notably lack any

---

2 Convention on Cybercrime (adopted 2001, November 23). ETS No. 185.

3 The UNGA. Resolution adopted by the General Assembly on 24 December 2024. UN Doc A/RES/79/243.

4 Obama, B. (2015, February 13). *Remarks by the President at the Cybersecurity and Consumer Protection Summit*. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

5 UN Charter, Article 2(4), Article 51; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 1986 [191].

6 *Nicaragua v US* [195].

Committee debate on defining an 'armed attack' (Brownlie, 1963, p. 275), suggesting the meaning of this concept was uncontroversial during the final stages of World War II. While factors like severity, immediacy, directness, and State involvement are proposed for assessment (Schmitt, 2017, hereinafter — *Tallinn Manual 2.0*, Rule 69 para 9), the inherently covert nature of cyber operations, along with their often delayed and non-physical consequences, make this practical application difficult. Consequently, States have developed divergent interpretive approaches. An 'effects-based' approach (championed by States like France[7] and the UK[8]) argues that severe economic or financial harm, even without physical damage, can constitute a use of force. An 'instrument-based' approach focuses on the means used, asserting that any tool, including cyber capabilities, can be used to violate the prohibition (Roscini, 2014, p. 47). A 'target-based' approach suggests that attacks on critical infrastructure could qualify (Roscini, 2014, p. 47), though this risks over-expansion without consensus on what constitutes 'critical' infrastructure. The threshold for an 'armed attack' is even higher, requiring the 'most grave' forms of force,[9] such as operations that cause death, serious injury, or significant destruction.[10] Ultimately, there is no international consensus, as evidenced by deadlock in the UN forums, leading States to default to a cautious 'case-by-case' analysis. This ambiguity is exacerbated by the potential for cyber operations to have long, cascading consequences and the significant risk that classifying them as armed attacks could escalate conflicts by justifying kinetic self-defence.

In the face of this uncertainty and at the same time political sensitivity of States' cybersecurity, this paper examines (i) the right to self-defence against cyber operations under Article 51 of the UN Charter, including the highly controversial issue of anticipatory self-defence against an 'imminent' cyberattack; and (ii) the States' efforts on cybersecurity cooperation under bilateral and multilateral treaties beyond the UN Charter, in particular within the North Atlantic Treaty Organization (hereinafter — NATO) and the Shanghai Cooperation Organization (hereinafter — SCO).

---

7 Ministère des Armées, France. (2019, October). *International Law Applied to Operations in Cyberspace*. . https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf, 7.

8 UK Ministry of Defence, Cyber Primer (2nd edn, 2016), Annex 1A – International Law aspects, 12.

9 *Nicaragua v US* [191].

10 Tallinn Manual 2.0, Rule 71 para 8.

1. State practice and legal uncertainty: applying Article 51 to cyber conflicts

As was discussed earlier in the Introduction, there is a debate about the circumstances under which a cyber operation might reach the 'scale and effects' of an armed attack triggering execution of the right to self-defence in accordance with Article 51 of the UN Charter. It is the victim State that bears the burden to prove that there was an armed attack against it as responding to an armed attack is one of the conditions for the legality of exercising the right to self-defence (Delerue, 2020, pp. 462-463). To date, no cyber operation has been qualified as reaching the 'armed attack' threshold because of their low intensity.

When referring to the victim State and its right to self-defence, two aspects of the requirements *ratione personae* should be considered: who may exercise the right to self-defence, and against whom. According to Article 51 of the UN Charter self-defence may be exercised individually or collectively which means that not only the State considering itself a victim of an armed attack can resort to self-defence, but also third States can intervene at the request of the victim (Randelzhofer & Nolte, 2012, pp. 1420–1421). The *travaux préparatoires* reveal that the Committee drafting the UN Charter aimed to reassure certain States that the Charter would not undermine existing or future regional collective self-defence agreements (Alder, 2013, p. 86). This explicit indication to collective self-defence in Article 51 is the legal basis, in particular, for invoking Article 5 of the North Atlantic Treaty, as will be discussed in more detail in the following section of the paper. At the same time, the existence of such a security cooperation treaty is not a prerequisite for collective self-defence — it can be done also on an *ad hoc* basis. The possibility of collective response to cyber operations is especially welcomed by States with limited cyber defence capabilities, which see it as a shelter to counter attacks in cyberspace (or to pre-empt potential ones) carried out by a State with advanced cyber capabilities. Among them is Estonia which indicates that being "very much dependent on a stable and secure cyberspace", it maintains its right "to respond to harmful cyber operations either individually or in a collective manner".[11]

The second aspect of the *ratione personae* application relates to the 'addressee' of the measures constituting self-defence. Several States have addressed the problem of self-defence against an attack conducted by a

[11] Kaljulaid, K. (2019, May 29). President of the Republic at the opening of CyCon 2019, Speech in Tallinn. www.president.ee/en/offiial-duties/speeches/15241-president-of-the-republic-at-the-openingof-cycon-2019/index.html.

non-State actor, and their positions differ. Thus, the US has signalled its position in the broadest possible terms: the "inherent right of self-defence against an actual or imminent armed attack in or through cyberspace applies whether the attacker is a State actor or a non-State actor".[12] Austria particularly elaborated its view in the position paper of April 2024: actions of non-State actors can amount to an armed attack if two conditions are met: "1) there is a 'transboundary element', e.g. the non-state actor operates from the jurisdiction of another state; and 2) the other state is harbouring or otherwise substantially supporting the operations of the non-state actor under its jurisdiction, or is unable, as a consequence of the complete absence of state authority and effective control over the respective territory, to prevent or suppress the non-state actor's operations".[13] Brazil, on the contrary, underlines that it is possible to invoke self-defence against actions of non-State actors only if they are attributed to a State (Brazil even specifies the basis of attribution: if "they are acting on behalf or under the effective control of a state").[14] Consistently, Brazil opposes the invocation of self-defence against cyberattacks by non-State actors on the basis that a State was 'unable or unwilling' to prevent an attack with transboundary effect. Brazil claims that, while such malicious actions might be considered serious crimes, they cannot be classified as 'armed attacks' because under current international law this term applies only to State-sponsored actions.[15] The affected State should take reasonable steps to stop the attack and hold the perpetrators accountable, and failure to do so could lead to international responsibility for the State, with the victim State having the right to seek peaceful remedies.[16] France shares the same approach.[17]

Indeed, in the literature on the right to self-defence, the concept of self-defence against a non-State actor not supported by a State received developments in the context of the fight against non-State terrorist groups after the events of 9/11 (see, e.g.: Murphy, 2002, p. 50; Ruys & Verhoeven, 2005, p. 289). However, in the cyber context, the position expressed by Brazil appears to be more balanced than the Austrian approach cited above. Considering the

---

12 The UN. (2021, July 13). Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by states submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. UN Doc A/76/136 (hereinafter — Compendium), 137.

13 Position Paper of the Republic of Austria: Cyber Activities and International Law. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Austrian_Position_Paper_-_Cyber_Activities_and_International_Law_(Final_23.04.2024).pdf, 8.

14 Compendium, 20.

15 Ibid.

16 Ibid.

17 Ministère des Armées, France, 9.

covert nature of activities in cyberspace and difficulties of attribution, establishment of the jurisdiction from which the attack was perpetrated and the technical ability of the territorial State to suppress the malicious activities is a non-trivial task, the failure to fulfil which (if the Austrian position is accepted) could lead to a significant escalation and threat to the international security system based on the UN Charter.

Apart from these requirements regarding *ratione personae*, there is a substantial condition for legality of self-defence: it should be necessary and proportionate.[18] The 'necessity' presumably means that a State must be unable to effectively defend itself against an imminent or ongoing cyberattack without resorting to force — essentially, it is about whether force is the only way to respond to the hostile action in cyberspace (Schmitt & Pakkam, 2024, p. 211). The 'proportionality' condition, on the contrary, refers to the amount of force employed for defence. Presumably, armed self-defence will not be considered proportionate if only collateral damage is minimised (Newton, 2014, p. 280).

The specific measures that constitute self-defence raise questions about their inherent nature. A common position is emerging among States that have addressed the issue: self-defence against a cyberattack may be exercised through either cyber or kinetic means, and conversely, cyber means may be employed in self-defence against a kinetic attack.[19] Poland has publicly outlined the rationale supporting this stance: "[d]eprivation of the right to respond to such a cyberattack with kinetic means could render the self-defence right illusory when the perpetrator of an armed attack is little dependent on its functioning in cyberspace".[20] It should be noted, however, that not all States with published national positions on international law in cyberspace — including, for example, Russia — have formulated an official stance on this specific issue.

Finally, there is a procedural condition: the measure applied as self-defence should be reported to the Security Council and should end once the Security Council has implemented measures to ensure international peace and security.[21] This requirement serves two purposes: first, to ensure the Council is

---

18 *Oil Platforms (Iran v. U.S.)* (Judgment) [2003] ICJ Rep 161, [43], [73]–[74], [76].

19 Position Paper of the Republic of Austria: Cyber Activities and International Law. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Austrian_Position_Paper_-_Cyber_Activities_and_International_Law_(Final_23.04.2024).pdf, 7; Estonia: Compendium, 30; Finland: International law and cyberspace. Finland's national positions. https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727, 7; Germany: Compendium, 43; Norway: Compendium, 73–74.

20 Ministry of Foreign Affairs of Poland. (2022, December 29). The Republic of Poland's Position on the Application of International Law in Cyberspace. https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace, 5.

21 Greenwood, C. (2011, April). 'Self-Defence' in *Max Planck Encyclopedia of Public International Law (MPEPIL)*.

aware of the conflict and informed of the affected State's actions, and second, to affirm the Security Council's legal authority (and responsibility) to act at any time to maintain or restore international peace and security (Alder, 2013, p. 85).

The question of the validity of the right to self-defence over time is related not only to the moment of its termination (taking measures by the Security Council), but also to its beginning. The most controversial aspect, especially in relation to potential cyber-enabled armed attacks, is the perennially debated issue of the right to preventive self-defence. Without delving into the rich and endless debate on the right to anticipatory self-defence in the general doctrine of international law (Kolb, 2003, pp. 192–193; Brownlie, 1963, pp. 258–260; Bowett, 1958, pp. 118–192), it should be noted that, with respect to cyber operations, there is no consistent State practice in a sense of a legal obligation to date that indicates support for possible preventive self-defence against cyberattacks. Certain States, on the contrary, have expressed concern about the possible extension of the right to self-defence as a preventive response to a cyberattack. Brazil, once again demonstrating careful wording, noted that the notion 'preventive self-defence' is not grounded on Article 51 nor on customary international law.[22] Germany, in its turn, specified that the requirement of Article 51 on the 'imminence' of an attack for self-defence to be lawful, applies also to malicious cyber operations, and therefore, "[s]trikes against a prospective attacker who has not yet initiated an attack do not qualify as lawful self-defence".[23]

While some unanimity can be noted in States' caution about the concept of anticipatory self-defence against a cyberattack, the question of when an attack is considered 'imminent' remains debated. One perspective, rooted in historical *Caroline* precedent, focuses on the time frame — meaning an attack is imminent if it is likely to happen soon.[24] The *Tallinn Manual 2.0* experts, however, concluded that this standard would be difficult to apply in cyberspace, as anticipating when a cyberattack might happen is challenging, and the effects of a cyberattack can emerge rapidly.[25] Instead, they referred to the test of 'the last feasible window of opportunity' developed by Michael Schmitt: a State can use anticipatory self-defence against an imminent cyberattack if delaying action would render it unable to defend itself effectively — the key factor is not the time frame, but whether waiting would make effective defence impossible when the

https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e401, 8. According to the ICJ, "the absence of a report may be one of the factors indicating whether the State in question was itself convinced that it was acting in self-defense" (*Nicaragua*, p. 105).

22 Compendium, 20.

23 Compendium, 43.

24 Letter from Daniel Webster to Lord Ashburton. (1842, August 6). Reprinted in 2 International Law Digest 412 (John Bassett Moore ed., 1906).

25 Tallinn Manual 2.0, Rule 73 para 3.

attack occurs.[26] State practice on this issue still has to evolve, however, the emerging views already show States' doubts. The African Union States labelled the question of self-defence against an imminent attack 'controversial' and deserving further study and deliberation between States, considering specific characteristics of cyber operations. The hesitation is based on the Union's position that "from a policy perspective, the maintenance of international peace and security favors the continued adoption of a restrictive interpretation of the exceptions to the prohibition on the use of force".[27] It is an opinion that is hard to disagree with.

The ongoing debate on application of the *jus ad bellum* norms in cyberspace got a second wind amid the increasing sophistication and autonomy of cyberattacks involving artificial intelligence (hereinafter — AI). A central challenge, however, lies in the inherent limitations of autonomous AI algorithms to evaluate the qualitative factors — such as the intensity of an operation — essential for an 'effect-based' assessment of use of force. This evaluation necessitates either extensive pre-programming or continuous human operator oversight to ensure compliance with the legal restrictions on the use of force, raising the question of whether AI can, in principle, ever autonomously assess the legality of an attack (Stroppa, 2023, p. 7). Moreover, the ramifications of autonomous cyber capabilities extend far beyond immediate physical destruction. Given the profoundly interconnected architecture of cyberspace, such operations risk triggering cascading systemic effects that could destabilise critical infrastructure, economies, and ultimately threaten human safety. Consequently, a comprehensive evaluation of potential collateral damage and long-term second-order effects is imperative for any legal assessment of their permissibility.

The lawful exercise of the right to self-defence under Article 51 of the UN Charter through AI necessitates that the system itself be capable of, first, accurately characterising a hostile cyber or kinetic operation as constituting an 'armed attack' and, second, formulating and executing a response that adheres to the core legal principles of necessity and proportionality.[28] Furthermore, a retaliatory 'hacking-back' operation mandates unequivocal attribution of the

---

[26] Tallinn Manual 2.0, Rule 73 para 4.

[27] African Union Peace and Security Council. (2024, January 29). Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, 42.

[28] On proportionality in the *jus as bellum* for autonomous cyber capabilities see Peter Margulies, 'Autonomous Cyber Capabilities, Proportionality, and Precautions' in: Liivoja, R., & Väljataga, A. (Eds.). (2021). *Autonomous Cyber Capabilities under International Law*. NATO CCDCOE Publications 2021. https://ccdcoe.org/uploads/2021/05/Autonomous-Cyber-Capabilities-under-International-Law.pdf, 162–165.

initial attack to a specific perpetrator to mitigate the significant risks of unlawfully employing force against a third State and incurring subsequent international legal responsibility for the responding State. The technical process of attribution is profoundly complicated by the use of obfuscation and mimicry technologies. This challenge is compounded by the fact that legal attribution — the act of imputing conduct to a State — is inherently a politico-legal determination, requiring a nuanced, contextual analysis that exceeds the current capabilities of autonomous AI systems.

As cyberattacks today are seen as fitting into the category of intrusions short of armed attacks, self-defence in the sense of Article 51 of the UN Charter remains an exceptional and, perhaps, still only theoretical mode of self-help of the State — victim of malicious cyber activities. This brings us to other (possibly, more practical) modalities of collective self-defence, based on bilateral and multilateral treaties.

2. Beyond the UN Charter: cyber defence of NATO and SCO

With the growing threat of hostile State actions in cyberspace, especially given the current geopolitical tensions, cooperation among States with common interests in international information security, or cybersecurity, plays a special role. The trend over the last decade of forming groups of 'like-minded' States and increasing coordination of their political course is also reflected in the formation of 'camps' of States on cybersecurity issues.

NATO member States have made the most progress in developing a collective position, reflected in international law documents, on countering cyber threats since 2002 when cyber defence first appeared in the political agenda of the organisation at the Prague Summit.[29] In 2010 cyber defence was included in the NATO Strategic Concept.[30] The Wales Summit Declaration of 2014, updated in July 2022, for the first time explicitly indicated that "[c]yber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. <…> A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis".[31] This vague statement without qualifiers of the intensity or the level of damage caused by an attack triggering response under Article 5 is explained by

[29] Prague Summit Declaration. (2002, November 21). https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2002/11/21/prague-summit-declaration.

[30] The North Atlantic Treaty Organization. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf.

[31] Wales Summit Declaration. (2014, September 5). https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2014/09/05/wales-summit-declaration, 72.

some commentators with reluctance of the Alliance "to weaken its position by revealing its red lines and reaction measures in cyberspace".[32] At the same time, NATO officials in their statements have admitted the possibility of applying Article 5 in the situation of an attack similar to the attack on Estonia in 2007 (Bryan & Smith, 2018, p. 42).

In 2016, at the Warsaw Summit NATO made a step further and recognised cyberspace as a 'domain of operations'.[33] Special attention is given to "close bilateral and multilateral cyber defence cooperation, including on information sharing and situational awareness, education, training, and exercises".[34] In the Brussels Summit Communiqué of 2021 the goal of "effective integration of sovereign cyber effects, provided voluntarily by Allies, into collective defence and Alliance operations and missions in the framework of strong political oversight" is declared,[35] however, without clarifications on how such integration is technically maintained. At the same time, the Communiqué recognises attribution of cyber activities as 'a sovereign national prerogative'[36] which suggests that, in the view of the authors of the document, countermeasures as a means of response can only be resorted to by the injured State. The Vilnius Summit Communiqué of 2023 develops the NATO commitment to counter cyber threats, including those potentially qualified as armed attacks, by strengthening collective deterrence and defense, enhancing resilience, and endorsing a new concept to better integrate cyber defense across all levels of the Alliance.[37]

The external cooperation of NATO is particularly close with the European Union. The NATO 2022 Strategic Concept, adopted at the Madrid Summit in June 2022, emphasises the need to enhance the 'strategic partnership' between the Alliance and the European Union, including in the task of 'countering cyber and hybrid threats'.[38] Cooperation contemplates exchange of cyber threat intelligence, joint training and research, as well as regulatory convergence. At

---

32 Prucková, M. 'Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO'. CCDCOE. https://ccdcoe.org/incyder-articles/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato.

33 The North Atlantic Council. (2016, July 9). 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. https://www.nato.int/cps/en/natohq/official_texts_133169.htm, 70.

34 Ibid, 71.

35 The North Atlantic Council. (2021, June 14). Brussels Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021. https://www.nato.int/cps/en/natohq/news_185000.htm, 32.

36 Ibid, 31.

37 The North Atlantic Council. (2023, July 11). Vilnius Summit Communiqué Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/07/11/vilnius-summit-communique.

38 NATO 2022 Strategic Concept. www.nato.int/strategic-concept/, 43.

the same time, episodes of unfriendly cyber-enabled actions between NATO partners in the past (including alleged surveillance of top European officials, including Angela Merkel, by US intelligence with Danish involvement[39]) underline once again that the pursuit of one's own political interests, including in the security field, often outweighs the desire to join forces against common external rivals.

On the other side of the globe, Russia and China are also taking steps to unite efforts in the field of information security, both bilaterally and under the aegis of BRICS and the SCO. As one of the first steps of cooperation, the bilateral agreement "On cooperation in ensuring international information security" was signed between the governments of Russia and China in April 2015 (hereinafter – the 2015 Agreement).[40] The 2015 Agreement contains a list of threats in the use of ICTs which include aggression aimed at the violation of the sovereignty, security, territorial integrity of States and a threat to international peace, security and strategic stability; causing economic and other damage, including through the provision of a destructive impact on the objects of the information infrastructure; terrorism; commitment of offenses and crimes, including those related to unauthorised access to computer data; interference in domestic affairs; dissemination of information which is considered harmful to the socio-political and socioeconomic systems, spiritual, moral and cultural environment of other States.[41] This list of ICTs threats demonstrates the difference in approach between the Russian-Chinese understanding of information security as a concept that includes threats related to information per se (including dissemination of information of undesirable categories) and actions against data, and the approach of NATO and the European Union, where the concept of cyber security is closely linked to the concept of cyber warfare, and the main threats in the field of cyberspace are seen in its use as a new testing ground or domain for inherently military actions.

As for the methods of cooperation between China and Russia under the 2015 Agreement, they are certainly far removed in their degree of integration from NATO's course on 'effective integration of sovereign cyber effects into collective defence'. The Russian-Chinese treaty contemplates 'softer' forms of cooperation such as exchange of information and cooperation in law enforcement to investigate cases involving the use of ICTs for terrorist and

---

39 Henley, J. (2021, May 31). Denmark helped US spy on Angela Merkel and European allies — report. *The Guardian*. https://www.theguardian.com/world/2021/may/31/denmark-helped-us-spy-on-angela-merkel-and-european-allies-report.

40 The Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security (adopted 2015, 8 May, entered into force 2016, August 10).

41 Ibid, Article 2.

criminal purposes; development and implementation of the necessary joint confidence building measures; cooperation between the competent authorities of the parties to ensure the safety of the critical information infrastructure; joint training of specialists, exchange of students and teachers from specialised higher education; conduct of meetings, conferences, seminars and other forums delegates and experts of the parties in the field of international information security.[42] The 2015 Agreement names, among the forms of cooperation, joint response to the threats in the field of international information security,[43] however, without elaborating on the modalities in which such response could be.

Interestingly, in a number of instances the 2015 Agreement provides for cooperation between Russia and China through the work of international organisations and fora (the UN, the International Telecommunication Union, the SCO, BRICS and others), as well as through other efforts to develop and promote international law in order to ensure national and international information security.[44] Indeed, the two States have, on a number of occasions, joined forces to promote a position within the work of the UN GGEs, as well as the efforts on development of a UN cybercrime convention. As part of BRICS, Russia and China signed the XIV BRICS Summit Beijing Declaration which underscored "the importance of establishing legal frameworks of cooperation among BRICS countries on ensuring security in the use of ICTs" and acknowledged "the need to advance practical intra-BRICS cooperation through implementation of the BRICS Roadmap of Practical Cooperation on ensuring security in the use of ICTs".[45] The XVI BRICS Summit Kazan Declaration calls for enhanced cooperation within the bloc to strengthen the security of and in the use of ICTs, the development of a universal UN-led cyber framework, and capacity building to ensure secure and equitable digital transformation, particularly for developing States, with a specific focus on the inadmissibility of unilateral actions undermining international cooperation in the cyber domain.[46] Besides, in 2011, four members of the SCO, including Russia and China, proposed to the United Nations General Assembly a Draft International Code of Conduct for Information Security. This initial proposal was later expanded to six members in 2015, with a revised version of the Code submitted to the General Assembly, but the core principles and content remained largely unchanged,[47]

---

42 Ibid, Article 3.
43 Ibid, Article 3(4).
44 Ibid, Article 3(3), (11).
45 XIV BRICS Summit Beijing Declaration. (2022, June 23). http://en.kremlin.ru/supplement/5819.
46 XVI BRICS Summit Kazan Declaration (2024, October 23). http://static.kremlin.ru/media/events/files/en/RosOySvLzGaJtmx2wYFv0lN4NSPZploG.pdf, 54.
47 UNGA. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. UN Doc A/69/273.

particularly with respect to the 'three evils' (terrorism, separatism and extremism) the fight against which is at the heart of the SCO foundation.

Overall, cooperation within the SCO, including in the sphere of information security, plays a special role for the States of Eurasia. The key regional international treaty in this area is the 'Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security' signed in Yekaterinburg on 16 June 2009 and entered into force on 5 January 2012 (hereinafter — the IIS Agreement).[48]

The IIS Agreement defines the main threats in the field of international and regional information security, which include the preparation and conduct of information warfare, cyberterrorism, and the use by individual States and corporations of a dominant position in the information space to the detriment of the interests and security of other States.[49] As the main areas of cooperation, the IIS Agreement provides, inter alia, for the establishment of a system for monitoring and joint response to threats arising in this area, countering threats of the use of ICTs for terrorist purposes, ensuring the information security of critical structures of the SCO member States, exchanging information on the legislation of SCO member States on ensuring information security, exchanging experience, training specialists, holding working meetings, conferences, seminars and conferences, as well as the exchange of data on information security issues.[50]

Despite the important role of the IIS Agreement in defining the general principles and areas of cooperation of the SCO member States in the field of information security, one cannot but note some shortcomings of this international treaty. Firstly, it is general and 'framework'-based (defining general principles rather than specific obligations of the parties), and secondly, some lagging behind the rapid development of technology that has occurred since 2009, when the text of the IIS Agreement was drafted (which makes some of its provisions quite incomplete today). Generally, obstacles to the effective cooperation in the field of international information security in Eurasia include a relatively low level of trust and a high level of competition for leadership in cyberspace (primarily between China and Russia). As ICTs today play a critical role in both the military and civilian sectors, the 'stakes' for overall national security are high, and States tend to be driven primarily by national interests rather than seeking cooperation.

---

48 The Shanghai Cooperation Organisation.The Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security (adopted 2009, June 16, entered into force 2012, January 5).

49 Ibid, Article 2.

50 Ibid, Article 3.

Overall, in the context of the almost open confrontation in the cyber-related discourse between the Western States, on the one hand, and Russia and China, on the other, there is hardly any prospect of rapprochement on the issues of legally binding norms of responsible State behaviour, including non-use of force, in cyberspace in the near future (with the exception of cybercrime issues). At the same time, treaty norms will continue to be adopted vis-à-vis ‘like-minded’ States: within regional unions and on a bilateral basis. However, the interpretation of the existing norms within the ‘like-minded’ States will lead to the fragmentation of their interpretation and hinder crystallisation of cyber-specific customary rules.

Conclusion

To date, there is a consensus in the official States positions on applicability of the norms and principles of international law, and particularly the UN Charter, in cyberspace. At the same time, questions remain about who can enforce the norms and principles of international law regarding cyber-enabled activities, how they should be applied, and in what specific circumstances. Inter-State cyber operations can potentially violate several primary rules of international law, including prohibition of the use of force, and give rise to the right to individual and collective self-defence. However, applying these rules to cyber activity is complicated and controversial. The increasing role of regional alliances — such as NATO and the SCO — in collective self-defence against cyberattacks indicates not only political division into the groups of ‘like-mended’ States, but also fragmentation of the interpretation of existing UN Charter norms and, potentially, the demand for more structured legal adaptation of the UN security framework.

The divergent State positions on applying *jus ad bellum* to cyber incidents — such as the 'effect-based', 'instrument-based', and 'target-based' approaches — reveal a lack of unanimity. This analytical challenge is compounded by the potentially extensive and prolonged chain of consequences triggered by a cyber operation compared to conventional force. While some cyber operations may constitute use of force, overextending the analogy with kinetic attacks risks contradicting the UN Charter's deliberate omission of non-physical coercion, like economic measures, from its express prohibitions. Consequently, a cautious and restrictive interpretation of exceptions to the prohibition of force — especially regarding self-defence against an 'imminent' cyberattack — is advisable from a policy perspective.

Список литературы / References

1. Alder, M. C. (2013). *The inherent right of self-defence in international law*. Springer.
2. Bowett, D. W. (1958). *Self-defence in international law*. Manchester University Press.
3. Brownlie, I. (1963). *International law and the use of force between states*. Oxford: Clarendon.
4. Bryan, E. D., & Smith, H. A. (2018). North Atlantic Treaty Organization: challenges to collective defense in cyberspace. *American Intelligence Journal*, *35*(2), 42–45.
5. Delerue, F. (2020). *Cyber operations and international law*. Cambridge University Press.
6. Jiang, C. (2021). Decoding China's Perspectives on Cyber Warfare. *Chinese Journal of International Law*, *20*(2), 257–312.
7. Kolb, R. (2003). *Ius contra bellum: Le droit international relatif au maintien de la paix*. Helbing Lichtenhahn & Bruylant.
8. Murphy, S. D. (2002). Terrorism and the concept of armed attack in Article 51 of the U.N. Charter. *Harvard International Law Journal*, *43*(1), 41–51.
9. Newton, M. (2014). *Proportionality in international law*. Oxford University Press.
10. Randelzhofer, A., & Nolte, G. (2012). Article 51. In B. Simma et al (Eds.). *The Charter of the United Nations: a commentary*. Oxford University Press.
11. Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford University Press.
12. Ruys, T. & Verhoeven, S. (2005). Attacks by private actors and the right of self-defence. *Journal of Conflict & Security Law*, *19*(3), 289–320.
13. Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
14. Schmitt, M. N., & Pakkam, A. S. (2024). Cyberspace and the jus ad bellum: the state of play. *International Legal Studies*, *103*, 194–229.
15. Stroppa, M. (2023). Legal and ethical implications of autonomous cyber capabilities: a call for retaining human control in cyberspace. *Ethics and Information Technology*, *25*, article number 7.