
**UNIVERSIDADE CATÓLICA PORTUGUESA**

# The Cyber Domain and the Use of Force

## A critical analysis to articles 2(4) and 51 of the Charter of the United Nations

Beatriz Garcia Sequeira

Faculdade de Direito | Escola do Porto
2024

**UNIVERSIDADE CATÓLICA PORTUGUESA**

# The Cyber Domain and the Use of Force

## A critical analysis to articles 2(4) and 51 of the Charter of the United Nations

Beatriz Garcia Sequeira

Orientador: José Alberto de Azeredo Ferreira Lopes

Mestrado em Direito

Faculdade de Direito | Escola do Porto
2024

To my mother, the woman of my life.

## Acknowledgements

I want to thank my family for being the most supportive and patient with me during the process of writing this thesis. To my brother, my biggest fan.

To my friends, that made this path less lonely.

I would also like to thank professor Azeredo Lopes, for the honour of working with him, and for every piece of valuable advice and knowledge.

## Resumo

Esta dissertação tem por objetivo analisar e comparar as diferentes posições dos Estados em relação ao uso da força no ciber domínio e o recurso aos artigos 2(4) e 51 da Carta das Nações Unidas.

No mundo em que vivemos, que é cada vez mais tecnológico, os Estados recorrem a armas e recursos ciber na sua agenda defensiva; desta forma, é importante entender a sua posição em relação ao uso da força através de meios ciber, e a possibilidade do uso da força em legítima defesa, no âmbito do artigo 51da Carta das Nações Unidas.

Assim, para a realização desta dissertação, diferentes posições de diferentes Estados com diferentes formas de ver o mundo foram analisadas. Consequentemente, pode concluir-se que a comunidade internacional concorda acerca da possibilidade de um ciberataque ter consequências que possam inserir-se na definição de um ataque armado, caindo, assim, no âmbito de aplicação do supramencionado artigo, ativando o direito à legítima defesa por parte do Estado atacado.

De notar ainda que este trabalho é importante na medida em que reúne informação acerca de diferentes Estados, com diferente História, culminando numa analise clara da sua posição relativamente ao problema mencionado anteriormente.

## Palavras-chave

Ciberataque; uso da força; agressão; artigo 4(2); artigo 51; legítima defesa.

## Abstract

This thesis aims to analyse and compare the different positions of States regarding the use of force in the cyber domain and the resource to articles 2(4) and 51 of the Charter of the United Nations.

In the world we are living in, which is more and more technological, States resource to cyber weapons and resources in their defensive agenda; therefore, it is important to understand their position regarding the use of force through cyber means and the possibility of resort to force in self-defence, under the umbrella of Article 51 of the Charter of the United Nations.

Thereby, for this thesis different positions of different States were analysed with distinct ways of seeing the world. Consequently, it's possible to conclude that the international community agrees upon the possibility of a cyber-attack having such consequences that one can consider it as an armed attack, thus falling under the scope of Article 51 of the Charter, triggering the right to self-defence of the attacked State.

This paper-work is important as it gathers information about different States with distinct backgrounds, and provides a clear analysis of their position regarding the previously mentioned problem.

## Keywords

Cyber-attack; use of force; aggression; article 4(2); article 51; self-defence.

## Abreviations

CAP – Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace.

CCDCOE – NATO Cooperative Cyber Defence Centre of Excellence.

CSIS – Center for Strategic & International Studies.

DoD – Department of Defence of the United States of America.

GGE – United Nations Group of Governmental Experts.

ICJ – International Court of Justice.

ICT – Information and communication technology.

IGE –International Group of Experts.

IHL – International Humanitarian Law.

IL – International Law.

LOAC – Law of Armed Conflicts.

NATO – North-Atlantic Treaty Organisation.

OEWG – United Nations Open Ended Working Group.

UN – United Nations.

U.S – United States of America.

WWII – World War II

## Index

## Cyberwarfare as a new domain

When Alexander Bell first patented the telephone in 1876[1], no one thought that less than 150 years later, someone would be putting wireless brain chips that allows them to control digital devices such as telephones and computers only with their minds[2].

In the same way as Archduke Franz Ferdinand could have not even dreamt about the existence and proliferation of modern weapons as nuclear and chemical weapons.

According to Monroe College[3], the very first cyberattack occurred in France, in 1834, when the French telegraph system was hacked to steal financial market information. Almost 100 years later, in 1940, Rene Carmille deceived the Nazis and disrupted their efforts to track down Jews through his information process machines; he was the first known ethical hacker[4].

Today the world has changed and we're living in a digital era, affecting all fields of our lives.

The NATO Wales Summit in 2014 was very important in terms of the agreement upon the relevance of cyber defence as one of NATO's core tasks of collective defence. At the same time, NATO's policy also recognises that International Law[5] applies in cyberspace[6].

Later, in Warsaw in 2016, NATO recognised that "cyber-attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack"[7]. Hence, NATO reaffirms its defensive mandate, recognising 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."[8]

Cyber warfare as we know it was first seen in 2010, with the world's first cyber weapon[9], Stuxnet, a malware that targeted the centrifuges in Iran's nuclear program. But for me, the kick-off was made much earlier, when the Soviet Union and the United States

---

[1] "Birth of telephone" (1899). Omaha Daily Bee, p. 6, available here: https://chroniclingamerica.loc.gov/lccn/sn99021999/1899-07-09/ed-1/seq-26/#words=Birth+Telephone

2 JACKSON Patrick; Tom GERKEN, BBC News. "Elon Musk says Neuralink implanted wireless brain chip" (30/01/2024).

3 Monroe College, "Cybersecurity history: hacking & data breaches" (2024).

[4] Also known as white hat hackers – hackers that do not have the objective of harming the system or a organization, but they do so to locate vulnerabilities, providing solutions to fix them.

[5] Including IHL and the UN Charter.

[6] See para. 72 of the Wales Summit Declaration of the 5th September of 2014. Available here: https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[7] See para. 70 of the Warsaw Summit Communiqué of the 9th July of 2016. Available here: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[8] See para. 70 of the Warsaw Summit Communiqué of the 9th July of 2016. Available here: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[9] According with Freeman Spogli Institute's Center for International Security and Cooperation. Article "Stuxnet: The world's first cyber weapon", available here: https://cisac.fsi.stanford.edu/news/stuxnet

engaged in a race to develop advanced computer technology. Later, in the 90's, as the internet became more widespread, the door was opened so that the world could walk (or run) towards what we have now.

This work aims at analysing the position of States before articles 2(4) and 51 of the Charter of the United Nations, as well as States' practices regarding a possible application of the mentioned articles to cyber warfare.

On the other hand, it is important to mention that this thesis obtains relevance and actuality thanks to recent efforts in the direction of universalization of certain positions, namely with the Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, adopted by the Peace and Security Council of the African Union.

The CAP reflects the position of the African Union's 55 States-members, outlining an important and unprecedent contribution to the progress of international cyber law. Moreover, the CAP may represent a turnover in a way that the international community can start to pay more attention to these countries' opinions and positions, that usually are not taken into account when discussing ground-breaking questions of IL. Having African States sitting at the table is something that really needs to start happening, and nothing better than begin with such an important and innovating field as it is this fifth domain.

Nationally, this work also gains significance in the light of the Portuguese Strategy for Cyberdefense, approved in November 2022. This Strategy highlights cyber security as a national priority and sets the pace for future national policies.

## Early definitions and clarifications

According to the National Institute of Standards and Technology, a cyber operation is "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace"[10].

On the other hand, "cyberattack refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks"[11]. However, the common definition of an armed attack cannot be mistaken with a cyber operation that under international law is considered an armed attack.

There are different types of cyber-attacks, with different kinds of intentions and effects. The International Journal of Advanced Computer Science and Applications of The Science and Information Organization mentions eight types of cyber-attack - Worms, Virus, Trojan Horses, DDoSs, Targeted Attacks, Whistleblowers, Denials of Service and Accounts Hijacking.

A Worm is, in terms of its propagation, like a virus, flowing through the network with no direction given by the attackers. Nevertheless, in worms, no interaction is needed from the user for their attempt to spread to be set in motion.

Differently, a Virus, and despite having the same means of propagation as a Worm, attaches its "body" to a target file (usually executable files, scripts, and documents); after the infected file is executed, the virus activates itself, running with it.

On the other hand, we have a Trojan Horse when, as the name says, the malware invades the computer by being disguised as a real and operational program. Once being in the computer, some trojan wait for the perpetrator to give them instructions, and some activate themselves alone[12].

DDoS stands for Denial of Service Attack, and represents a coordinated attack on the system service availability that has been given to the target; this means that this kind of attack floods the system of the target, overwhelming it[13].

---

[10] Definition available here: https://csrc.nist.gov/glossary/term/cyberspace_operations.

[11] National Research Council, et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilitie.s* The National Academies Press. (2009). P.1.

[12] McAfee, "O que é um vírus trojan e como remover" (2021). Available here: https://www.mcafee.com/blogs/pt-pt/internet-security/compreender-os-virus-troianos-e-como-se-livrar-deles/

[13] CloudFlare, "What is a DDoS attack?" (2024). Available here: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

The Targeted Attacks are directed to a particular individual, software, system or company because there is a particular interest in that very person or infrastructure.

In addition, a Whistleblower Attack refers to the disclosure of information that uncover perceived wrongdoing within the organization or the company; it can also aim at individuals or entities that have the power to affect that organization's or company's actions.

A Denial of Service interrupts the device's or the network normal functioning, normally through a flood of requests to the target, until they're unable to be responded[14].

Lastly, an Account Hijacking is a process where a particular individual's computer or any account is hijacked or stolen by hackers.

Regarding intention, it can be to provoke the loss of human life or the destruction of property; it can also be to disrupt the flow of activity of the system or to provoke a service delay; on the other hand, the purpose can even be to extract sensitive data or having political repercussions. But this is not an exhaustive list.

[14] CloudFlare, "What is a denial-of-service attack?". Available here: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

## The applicability of the IL to the cyber domain

The first question that needs to be answered is whether the International Law applies or do not apply to cyberspace and cyber warfare. If a few years ago this could impose many problems, nowadays it is pacific that International Law rules do apply to cyber operations; it is not a legal vacuum.

Despite some exceptions[15], the real question today is how to apply international law to the cyber context. The position the International Law do apply to cyberspace has been taken by numerous relevant institutions, such as the G20[16], the European Union[17] and the OAE[18].

NATO in its 2014 Wales Summit has agreed that IL is applicable to the cyberspace, and that cyber defence is part of its primary objectives regarding collective defence purposes. Moreover, the EU's Cybersecurity Strategy for the Digital Decade has already reaffirmed the cyber space as an important military domain[19].

Many States have already stated that IL and in specific IHL do apply to cyberspace. For instance, the United States in its Submission to the UN GGE has already asserted that "the challenge is not whether existing international law applies to State behaviour in cyberspace (…) international law does apply, and such law is essential to regulating State conduct in this domain."[20] Earlier, in 2011, Barack Obama also concluded that "[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete."[21]

[15] Such as the Council of Europe Budapest Convention on Cybercrime.
[16] That has stated that "the international law, and in particular the U.N.Charter, is applicable to state conduct in the use of ICTs". Antalya Summit, G20 Leaders Communiqué (2015). Para. 25. Available here: https://www.gpfi.org/sites/gpfi/files/documents/G20-Antalya-Leaders-Summit-Communiqu--.pdf.
[17] Which "emphasises that (...) the U.N (…) have reached consensus on a number of measures contributing to greater cyber stability, including (…) the application of international law in cyberspace". EU Statement – United Nations 1st Committee: Thematic Discussion on Other Disarmament Measures and International Security (2018). Available here: https://www.eeas.europa.eu/node/52894_en.
[18] That in its Resolution AG/RES. 2959 (L-O/20) (2020) reaffirmed "the applicability of international law to cyberspace". Para. i. Available here: http://www.oas.org/en/sla/iajc/docs/AG-RES_2959_EN.pdf.
[19] Available here: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.
[20] See the United States Submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015).
[21] See Barack Obama, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, 9 (May 2011).

## The LOAC Manuals

The Spanish LOAC Manual implicitly agrees with the application of the existent IHL, when saying in its Chapter 4 that, given the lack of experience and jurisprudence, the whole chapter dedicated to the cyber domain is based in doctrinal references, States practice and the existent rules of IL[22].

The Norwegian LOAC Manual also provides that the LOAC applies to the cyber domain, recognizing, nevertheless, the challenges that this application can pose to the international community[23]. Furthermore, the Danish LOAC Manual agrees with the international community, treating the Computer Network Operations[24] "as a means of combat subject to the existing rules of international law."[25]

In addition, the French LOAC Manual also states clearly that the international law is applicable to the cyber domain[26]; likewise, also Sweden is of the opinion that new rules regulating cyber activities are not needed. Notwithstanding, Sweden recognises that "cyber technology may give rise to specific questions requiring further clarification." [27].

The New Zealand LOAC Manual also provides that, even though there is no specific treaty obligation relating to the conduct of warfare through electronic means, "the principles of LOAC apply to all military operations, regardless of the medium employed"[28] [29].

---

[22] Derecho internacional humanitario (DHI) en las FAZ (2022). "gran parte del contenido de este capítulo se basa, em buena medida, en referencias doctrinales y práctica de los Estados así como, en lo referente al conflicto armado, en la adaptación del marco existente (el DIH) al supuesto de las operaciones en el ciberespacio." Chapter 4. Para. 4.2. Available here: https://ihl-databases.icrc.org/en/national-practice/all-national-practice?title=&typeOfPractice=18553&state=17916&language=&from=&to=&sort=country&order=&topic=.

[23] "There is international agreement that the law of armed conflict also applies to cyber operations, although its application in practice may pose certain challenges."
Chapter 9. Para. 9.50 of the Manual of the Law of Armed Conflict (2013). Available here: https://usnwc.libguides.com/ld.php?content_id=47416967.

[24] Also known as Cyber Operations.

[25] Chapter 3. Para. 3.10. p. 96 of the Military Manual on international law relevant to Danish armed forces in international operations (2020). Available here: https://www.forsvaret.dk/globalassets/fko---forsvaret/dokumenter/publikationer/-military-manual-updated-2020-2.pdf.

[26] "Le droit international est applicable aux cyberopérations".
Chapter 4. P. 295. Manuel de droit des opérations militaires (2022). Available here: https://www.defense.gouv.fr/sites/default/files/sga/Manuel%20de%20droit%20des%20opérations%20militaires_édition%202022.pdf.

[27] See Position Paper on the Application of International Law in Cyberspace (2022). P. 1. Available here: https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf.

[28] New Zealand Manual of Armed Forces Law (2019). P. 39. Para. 8.10.23. Available here: https://usnwc.libguides.com/ld.php?content_id=47364407.

[29] This Manual refer many times to the Tallinn Manual 2.0, following and accepting its Rules and positions. See for example, footnotes in page 39 of the LOAC Manual.

## Other States opinions

Notwithstanding not having its own LOAC Manuals, many countries have already made its position public, regarding the applicability of the IL to the cyber domain.

Czech Republic, for a start, being "aware of the opportunities and threats arising from the technological progress in information and communication technologies", fully recognizes that the IL apply to cyberspace; it constitutes "a fundamental element of the framework for responsible State behaviour in cyberspace, which is essential to maintaining international peace and security, including in relation to cyber activities"[30].

On the other hand, Estonia has submitted its national position regarding this issue, and "reiterates that existing international law applies in cyberspace"[31]. The Estonian State has considered that IL "provides a solid normative framework for state actions, regardless of the means or the environment for these actions"[32].

China has also presented its vision[33], and is of the opinion that principles of IL such as sovereign equality and the prohibition of the threat or use of force do apply to the cyber context. "The application of these principles is the cornerstone of the peace, security and stability in cyberspace."[34]

Russia has given its opinion too. It has assumed that IL apply to cyber operations, but, at the same time, enhances that given the "specific legal nature of the information environment, notably, the fact that activities therein can be anonymous"[35], the IL must not be applied automatically.

Iran back in 2020 has also published its official opinion, agreeing with the other countries upon that IL really applies to the cyber domain. This position prepared by the

[30] Czech Republic Position Paper on the application of international law in cyberspace (2024), presented by collaboration of the Ministry of Foreign Affairs of the Czech Republic, the Ministry of Defence of the Czech Republic, and the National Cyber and Information Security Agency and approved by the Committee for the Foreign Security Policy Coordination. Available here: https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf.

[31] See the National position of Estonia (2021), which is also part of the official UNGGE compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States. Available here: https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.

[32] See the National position of Estonia (2021).

[33] Through the Ministry of Foreign Affairs, in October 2021.

[34] China's Positions on International Rules-making in Cyberspace, Ministry of Foreign Affairs of the People's Republic of China. Available here: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1915533.shtml.

[35] Russia's Position of the application of the IL to cyberspace (2021), present in the Official Compendium of the UN GGE, referred previously in footnote 32. See pp. 79-80.

Armed Forces Cyberspace Centre and published by the General Staff of the Iranian Armed Forces goes in the same way of the majority of States.

More than 30 countries[36] have published its opinion regarding this issue, and they all go in the same direction: IL do apply to cyberspace. To these opinions we can now add the position of more than 50 African States; the Common position of the African Union reaffirms that IL applies and governs the use of ICTs in cyberspace. As mentioned above, this is an important step towards universalization, contributing to a more wide and plural international cyberspace law.

For its part, and despite not having a LOAC Manual, the government webpage of Canada also refers to the question of application of the international law to the cyber domain. Therefore, "Canada affirms that international law applies to the activities of every State in cyberspace"[37], namely the Charter of the UN and customary international law.

[36] Such as Australia, Brazil, Costa Rica, Estonia, Finland, Germany, Ireland, Israel, Japan, Kazakhstan, Pakistan, Singapore, Switzerland and The Netherands.

[37] "International Law applicable in cyberspace" (2022). Available here: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a2.

## The Tallinn Manual 2.0 and the GGE and OEWG

The Tallinn Manual 2.0 acquiesce to the same position. This Manual expatiates international law applicable to cyber operations, and starts on the assumption that international law is, indeed, applicable to this fifth domain[38]; the aim of this manual is to clarify and examine how extant legal rules apply to this new form of warfare.

Regarding this issue, both the UN GGE and the UN OEWG[39] have already confirmed the applicability of IL to the cyber context. And the reports of both have been adopted by the UN General Assembly[40].

With the intention of understanding the extent of these reports, it is important to apprehend its motivations and origins. It was back in the 90's[41] that the Russian Federation first asked the UN to address the issue of "Developments in the field of information and telecommunication in the context of international security" in its agenda.

Some Russian proposals were asking for an international treaty restricting military uses of cyber technology; nevertheless, these approaches were strongly rejected by the Bush Administration.

Despite this, these Russian proposals reunited enough support amongst the UN members; starting to show some concerns about the need for examination of the new technologies and its implications, a GGE was established for the period of 2003-2004, counting with 15 State-Members of the UN.

A Group of Governmental Experts – GGE, is a much common UN mechanism, that aims at studying new fields and subjects, with the purpose of creating recommendations that should influence future negotiations of different kinds[42].

Given the fact that this mechanism is based off in consensus, the first GGE was unsuccessful; unanimity could not be reached. However, the GGE process continued; a position that clearly shows the growing concern of the States regarding malicious cyber activity undertaken by cyber criminals or by State-actors.

---

[38] In addition to land, air, sea and space. The Netherlands Ministry of Defence, Defence Cyber Strategy (2012).
Available here:
https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/Netherlands_2012_NDL-Cyber_StrategyEng.pdf.

[39] Report of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N.Doc. A/68/98 (2013); Report of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N.Doc. A/70/174 (2015); Report of the GGE on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, U.N.Doc. A/76/135 (2021).

[40] Resolutions A/RES/68/243, A/RES/70/237, A/RES/76/19.

[41] In the year of 1998.

[42] E.g. negotiations for a multilateral agreement.

Thereby, a series of GGE were very successful: 2010, 2013 and 2015. In its 2013 Report, the GGE introduced the already mentioned conclusion that international law is indeed applicable to the novel domain of cyberspace and that it was "essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment"[43].

The 2015's Report was the first to extend the participation from 15 State-members to 20, which was motivated by the growing demanding by States for participation. As soon as this latter report was published, the UN General Assembly authorised a further GGE between 2016 and 2017, which would count with 25 participants.

Despite the last three GGEs being a success[44] the GGE of 2017 was an absolute failure. The increasing tension between specifically the U.S.A and, on the other side, Russia and China[45] came to surface with the GGE; the apparent motive for this breakdown was disagreement over how international law is to apply to state cyber activity. Despite not being successful, some participants of the GGE still raised their voices, which was the case of Miguel Rodríguez[46], Representative of Cuba, who suggested that by recognising "the supposed applicability in the context of ICT of the principles of International Humanitarian Law" the International Community is legitimising "a scenario of war and military actions in the context of ICT."[47]

After this outcome, in 2019 Russia presented another proposal, this time leaving the GGE formulation behind. It proposed the establishment of an Open-Ended Working Group – OEWG, a forum in which any interested State-member can be part. This OEWG was supposed to elaborate a Report, to be public in 2020.

The result was that both GGE and OEWG were approved, generating a duplication of mechanisms, both working for the same purpose. Although being a normal anathema

---

[43] See para. 19 of the GGE Report of 2013 (24 june 2013). Available here: https://dig.watch/wp-content/uploads/A_68_98_E.pdf. The same position was reiterated later, in the 2015's Report (see para. 24 of the GGE Report of the 22 July 2015). Available here: https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf?token=T0am0LEin9vyNIjWNS&fe=true.

[44] Through the years, the GGE recommended 11 voluntary, non-binding norms for responsible State behaviour.

[45] Namelly since the Russian action in Crimea in 2014.

[46] At the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security, in the 23rd June of 2017.

[47] "71 UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security" (2017). Available here: http://misiones.cubaminrex.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information.

in multilateral diplomacy, some logical division of labour should be created for the two processes to coexist and produce useful results.

The GGE's 2021 Report reaffirms the assessments and recommendations on international law of the reports of previous GGEs, notably that international law, and in particular the Charter of the United Nations are applicable and essential to maintaining peace and stability and for promoting an open, secure, stable, accessible, and peaceful ICT environment. These assessments, emphasised that adherence by States to international law, particularly their Charter obligations, is an essential framework for their actions in their use of ICTs.

The OEWG is a milestone towards international cooperation for an open, secure, transparent, attainable, and serene ICT atmosphere. It emphasised in its Report that international law and, in specific, the Charter of the U.N. is not only applicable, but also essential to maintaining peace and stability, and to promoting an "open, secure, stable, accessible and peaceful ICT environment."[48] Hence, the States should forbear and avoid taking any conducts not in accordance with international law. But what are the consequences to when a State actually acts against international law in the ICT field?

[48] Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report (10th March 2021). Para. 34. Available here: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

## The use of force and the cyber domain

### Initial considerations

The milestone regarding the prohibition of the use of force in international law must be Article 2(4) of the U.N Charter; “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”[49]

The Covenant of the League of Nations declared in its article 10 that "any war or threat of war" was dangerous to the entire community.”[50] Article 2(4) is an echo of this concern. The development of the Article in question continued during WWII; in 1941, Great Britain and the United States declared that "they believe that all nations of the world, for realistic as well as spiritual reasons must come to the abandonment of the use of force.”[51] In 1945, with the signature of the Charter of the UN, article 2(4) was already well established amidst the International Community.

[49] United Nations’ Charter. Article 2(4). Available here: https://www.un.org/en/about-us/un-charter/full-text.
[50] GORDON Edward, Article 2(4) in Historical Context. P. 273. Available here: https://core.ac.uk/download/pdf/72839491.pdf.
[51] Point Eight of the Atlantic Charter (1941). Available here: https://avalon.law.yale.edu/wwii/atlantic.asp.

## The Article's mechanic

Article 2(4) is, first and foremost, a norm of customary law[52] [53] [54]. In addition, it is also a formal treaty obligation; and States cannot simply walk away from their treaty's obligations.

This article enshrines a general prohibition of the resource to force. The ICJ, in its Nicaragua Case, found that the obligation to absence of threat or use of force has a binding character[55];. The opinio iuris as to this character can be deducted from, inter alia, the attitude of the Parties and of States towards the General Assembly resolution 2625 (XXV)[56].

The reference in article 2(4) to "threat or use of force (…) in any other manner inconsistent with the Purposes of the United Nations"[57], was intended to create a presumption of illegality for any threat or use of force. That is, even though not being against either the territorial integrity or the political independence of a State, an act may be unlawful, if inconsistent with the purposes of the United Nations. The intent of the authors was for article 2(4) to be as broader as possible regarding its scope; it is intended to prohibit almost every use of inter-state armed violence.

As a member of the United States Delegation stated, "[T]he intention of the authors of the original text was to state in the broadest terms an absolute all-inclusive prohibition; the phrase "or in any other manner" was designed to ensure that there should be no loopholes."[58]

We could consider that pre-Charter rules still apply nowadays, side by side with article 2(4). But they do not. Those ancient rules on the use of force did not include a general prohibition as it is now incorporated in the article; both the Covenant and the

[52] E.g., the U.N.Group of Governmental Experts 2013 Report (para. 19) and the 2015 Report of the same group (para. 25 and 26). Available here: https://digitallibrary.un.org/record/753055 and here: https://undocs.org/Home/Mobile?FinalSymbol=A%2F70%2F174&Language=E&DeviceType=Desktop&LangRequested=False.

[53] In its article 38, the ICJ's Statute describes customary law as "general practice accepted as law"; it requires the existence of State practice and the belief that the practice is based in a legal obligation.

[54] In the Nicaragua Case, the parties stated that "the Charter provisions represented customary law, and even jus cogens, and the Court accepted". GRAY Christine. "International Law and the Use of Force" (2018). P. 12.

[55] See Nicaragua Case (26th november 1984). Para. 73. Available here: https://www.icj-cij.org/sites/default/files/case-related/70/070-19841126-JUD-01-00-EN.pdf.

[56] Entitled "Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations". Available here: https://digitallibrary.un.org/record/202170.

[57] Article 2(4) oof the U.N.Charter, available here: https://www.un.org/en/about-us/un-charter/full-text

[58] Documents of the United Nations Conference on International Organization, vol. 6 (San Francisco, 25 April 1945), pp. 334–335.

Kellog-Briand Pact[59] only prohibited the war of aggression, allowing the States to act in numerous instances.

According to Natalino Ronzitti there are two possible interpretations of the article. Firstly, a broad interpretation. Article 2(4) has a "blanket prohibition"[60], meaning that the use of force is only allowed under strict specifications, hence, the established exceptions.

Nonetheless, a narrower vision was also considered, back in the period immediately following the entry into force of the UN Charter. According to this view, article 2(4) contains a qualified prohibition. Therefore, force, to be prohibited, must infringe the territorial integrity or the political independence of a State or be contrary to a concrete purpose of the UN. Thereby, there were some actions that, even though entering into a state's sovereignty domain, do not violate its territorial integrity nor political independence.[61] In addition, the ones defending this perspective, considered that in some cases, the use of force was in line with the purposes of the United Nations[62].

Despite this, most of the international community is of the opinion that article 2(4) enshrines a general ban of the use of force. For that reason, and because the tendency is to agree with this position, it is relevant to address the exceptions accepted as justifications to a use of force in international law.

This article was very much a response to the WWII, notwithstanding its scope being one of the most controversial fields of international law. The use of force is, indeed, a polemic theme in the international community, and has been motive of dispute between states over time[63]. These disagreements are as whether the use of force should or should not apply to economic coercion, the right to use force to further self-determination or to interfere in civil wars, and even the scope of the right to self-defence. The proliferation, in the last years of the XX century and first years of the XXI century, of groups such as Al-Qaida or ISIS have increased the already existent questions about the scope and length of the right to the use of force.

---

[59] Available here: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjDmLesrbyEAxV1U6QEHYv_BMgQFnoECBUQAQ&url=https%3A%2F%2Floveman.sdsu.edu%2Fdocs%2F1928KelloggBriand.pdf&usg=AOvVaw0reAJtBWt2zfVEQpFIWyaS&opi=89978449.

[60] RONZITTI Natalino. The current status of the principle prohibiting the use of force and legal justifications of the use of force (2002). Para. 2. Available here: https://www.iai.it/sites/default/files/iai0215.pdf.

[61] E.g. entering another State's territory to rescue nacionals.

[62] E.g. entering a foreign territory to put an end to a policy of genocide.

[63] Namely between Eastern and Western countries.

Some scholars[64] understand that legal rules must be 'realistic', meaning that these rules do not constrict the use of force by powerful states when applied against terrorist organisations, or to prevent the escalation of nuclear weapons. This approach seems a way of the authors rationalise and even try to justify their own State's actions, by trying to reconcile its use of force with the UN Charter.

It is important to enhance that the scope of 'force' has been discussed between scholars through time; some of them defend a narrower ambit than others. On the one hand, some jurists understand that the term refers solely to armed force, excluding, for example, economic force. On the other hand, scholars like Hans Kelsen defend that the definition of 'force' is wider, including any illegal action of a state that violates the interest of another, and not just armed force. At the same time, the first position considers that only traditional kinetic weapons can produce damage that may fall within the scope of article 2(4); on the contrary, opinions like the one presented by Kelsen, consider other types of weapons.

According to the ICJ, that in its Nuclear Weapons Advisory Opinion stated that article 2(4) and article 51 of the Charter do apply regardless the weapon used[65]. This is the outlook which allows analysing cyber operations under the scope of these articles. If we were of the view that only traditional kinetic weapons could trigger article 2(4) and 51, this study would have not been possible. We have already exposed our position, and we do agree that it is entirely possible for a cyber operation to qualify as a use of force.

[64] Such as the former UK's Foreign and Commonwealth Office Adviser Daniel Bathlehem or the former U.S Department Legal Adviser Harold Koh.

[65] ICJ Nuclear Weapons Advisory Opinion (1996). Para. 39. Available here: https://www.icj-cij.org/sites/default/files/case-related/95/095-19960708-ADV-01-00-EN.pdf.

## The Tallinn Manual 2.0

According to the Tallinn Manual 2.0, "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[66].

Hence, the threshold is the scale and effects of the cyber operation; this differs from the Charter, which is based on the instrument of coercion. At the time the Charter was drafted, the approach built around the instrument made sense, as one was only dealing with traditional kinetic operations. However, cyber operations do not fit in this paradigm; they are non-kinetic, despite their effects may range from mere inconvenience to death.

To understand what kind of attack constitutes a use of force, different proposals were raised. Firstly, an approach that applies a 'strict liability test' to any cyber operation that target a State's critical infrastructure or its pivotal interests. Also known as 'target-based' approach[67], the mere penetration of critical infrastructures or systems of a State constitutes evidence of hostile intent and may trigger the right to self-defence.

However, as pointed out by Andrew Foltz[68], this framework suffers from the inherent subjectivity of defining what constitutes "critical infrastructure and vital interests"[69], expanding the grey area already existent in this field.

Secondly, the 'kinetic equivalency' approach[70], which defends that a cyber operation will only be considered a use of force when its damage could previously have been achieved only through a kinetic attack. Again, it struggles with the so-called grey areas.

Lastly, the one adopted by the IGE in the Tallinn Manual 2.0, an 'effects-based' approach[71], which defends that is the quantum of damage, the consequences, of the attack that matters, and not the means through which it is made. This approach acknowledges that nations are mainly concerned about the consequences of cyber-attacks. Nonetheless, it relies on inherently subjective assessments among states that have different ways of seeing things, with diverse strategic interests, vulnerabilities, and capabilities.

---

[66] Schmitt, M. N. (2013). Short form citations. In Tallinn Manual on the International Law Applicable to Cyber Warfare (p. 330). list, Cambridge: Cambridge University Press.
[67] See https://dergipark.org.tr/en/download/article-file/1175613. P. 50.
[68]Lieutenant Coronel Andrew C. Foltz.
[69]FOLTZ C. Andrew. Join Force Quarterly. "Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate", issue 67, 4th quarter 2012. p. 42. Available here: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf.
[70]Which usually adheres to the Charter's instrument-based approach
[71]Also called Scmitt Analysis. Other authors have proposed similar approaches; Richard Clark in his book "Cyber War: The Next Threat to National Security and What to Do About It" (2010) proposes a doctrine of "cyber equivalency", in which the cyber attacks are evaluated by its effects and not by its means.

As follows, there is no internationally recognised definition of a use of force. What does exist is a consensus regarding the fact that some cyber operations amount, effectively, to a use of force. Other cases are situated in a grey area, and for these it is necessary some kind of criteria, to assess whether we are facing an unlawful use of force. Even though the Charter does not refer any criteria, in Nicaragua Case, the ICJ stated that Scale and Effects is to be considered when assessing whether specific actions amount to an armed conflict.

In the Tallinn Manual 2.0, the IGE follows an approach near to the Schmitt Analysis, and refers some criteria that, despite not being exhaustive[72], should influence the States in the decision making regarding this manner. The Experts mention criteria such as severity, immediacy, directness, invasiveness, measurability, presumptive legality, State involvement and the military character. As shown, the Tallinn Manual 2.0 tends to follow the same direction as the ICJ: Scale and Effects is an important criterion when determining if a cyber operation entail a use or threat of use of force.

An important distinction to do is between 'use of force' and 'armed attack'. The latter is the threshold at which a State may use its right to self-defence under article 51 of the Charter. According with the ICJ in the Nicaragua Case, an armed attack is the "most grave" form of a use of force[73]. Thus, the IGE agreed in the Manual that all armed attacks qualify also as uses of force.

A contrary view argues that any unlawful use of force qualifies, per si, as an armed attack, triggering the right to self-defence. Thereby, no gap exists between the two concepts, and the response of the attacked State would only be limited by the principles of proportionality and necessity.

[72]It is not exhaustive, and do not wish to be exhaustive. Other examples of criteira can be the identity of the attacker or the political environment.

[73] Nicaragua Judgement, para. 191. Available here: https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

## The LOAC Manuals

### U.S LOAC Manual

This is the view of the U.S, that as long taken this position, considering that "the inherent right of self-defense potentially applies against any illegal use of force"[74]. On the other hand, the U.S LOAC Manual uphold that there is no legal requirement of a cyber response to a cyber-attack; the inherent self-defence principle is only mediated by the principles of proportionality and necessity.[75]

It is also relevant to refer those cases that do not amount to a use of force, despite being coercive acts. When drafting the UN Charter[76], States rejected a project to include economic coercion as a use of force. Neither non-destructive cyber psychological operations intended to compromise confidence in a government, nor merely funding guerrillas engaged in operations against another State reach the threshold of a use of force[77]. Therefore, funding a group of hacktivists conducting cyber-attacks as part of a rebellion should not be considered as a use of force against the State involved.

The DoD LOAC Manual refers to these kinds of operations and has ruled that albeit not being able to trigger the right to use force in self-defence, these cyber operations may justify those attacked States in taking necessary and appropriate measures in response[78].

Despite of article 2(4) of the Charter only applying to Members of the UN, this prohibition also extends to other States that are not part of the UN, by virtue of customary international law. Nevertheless, this does not apply to non-State actors, unless the conduct can be attributed to a State, through the law of State responsibility. Notwithstanding being unlawful under both international and national law, it cannot be seen as a violation of the prohibition of the threat or use of force.

The north American Manual also concerns about this question and says that a State's right to self-defence is not precluded by the fact that the perpetrator is a non-State actor. Therefore, the right to self-defence is entirely applicable to the actions of a non-State agent.

---

[74] DoD Manual, p. 1030, para. 16.3.3.1. Available here: https://tjaglcspublic.army.mil/documents/27431/61281/DoD+Law+of+War+Manual+-+June+2015+Updated+Dec+2016/5a02f6f8-eff3-4e79-a46f-9cd7aac74a95.

[75] Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), reprinted in 54 Harvard International Law Journal Online, 4 (Dec. 2012).

[76] In the San Francisco Conference (1945), in the United States.

[77] Nicaragua Judgement, para. 228: "the Court considers that the mere supply of funds to the contras, while undoubtedly an act of intervention in the interna1 affairs of Nicaragua, as will be explained below, does not in itself amount to a use of force". Available here: https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

[78] Measures that do not amount to a use of force, such as diplomatic protests or economic embargo.

The U.S. LOAC Manual clearly adopts the position of the UN Charter regarding the use of force: it prohibits cyber operations that constitute unlawful uses of force under article 2(4); it recognises that under certain circumstances, cyber operations may constitute uses of force, falling into the scope of the mentioned article[79].

**Spain LOAC Manual**

The Spanish LOAC Manual on the other hand, has a whole chapter dedicated to the use of force, which is specified as "every form of physical coercion"[80]. This Manual closely follows the Tallinn Manual 2.0, tending to agree with it. For instance, in Chapter 4.3.2, after giving a small and direct definition of what they understand as use of force, the Manual expound Tallinn's definition, giving us hints that they would follow the position of the Tallinn's Manual.

The Spanish LOAC Manual adds that, despite these definitions[81] that only refer physical damages, it is also possible for an operation to be an armed attack even without producing damage or the destruction of an object; this occurs when a cyber operation is not limited to communications, messing with the functioning of cyber infrastructures.

On the contrary, legal scholars understand that cyber operations that spread propaganda or espionage; cyber operations with similar consequences as economic penalties, as long as they do not affect indispensable infrastructures; and the ones aimed to interfere with civilian communications are not armed attacks[82].

**Norway LOAC Manual**

The Norwegian LOAC Manual, for its part, states in Chapter 9 that cyberattacks are subject to "the same restrictions and regulations as other types of attacks."[83] They define 'attack' as an act of violence against the enemy; however, the term 'violence' should not

[79] The Manual gives us some examples of cyber operations that can amount to a use of force; "cyber operations that: (1) trigger a nuclear plant meltdown, (2) open a dam above a populated area, causing destruction or (3) disable air traffic control services, resulting in airplane crashes." DoD Manual, P. 1028-1029, para. 16.3.1.

[80] "Derecho Internacional humanitario (DIH) em las FAS". P. 110, par. 31. Available here: https://publicaciones.defensa.gob.es/media/downloadable/files/links/p/d/pdc_02.01_derecho_internacional_humanitario_fas.pdf

[81] Referring to the ones given by the Tallinn Manual 2.0 and by the Protocol I (1977) of the Genebra Conventions of 1949.

[82] Radio or television communications.

[83] Manual of the Law of Armed Conflict (2013). P. 209. Para. 9.53. Available here: https://usnwc.libguides.com/ld.php?content_id=47416967.

be interpretated literally, so it can also cover acts with indirect violent consequences. Additionally, it describes a cyberattack as a cyber operation expected to provoke death or injury to people or destruction or damage to objects.

Given the fact that this Manual wants to apply its general considerations to the cyber domain, it is important for us to look to its considerations regarding the basic prohibition against the use of force. The Norwegian Manual build its approach around the consideration that the general prohibition of the use of force is based off on the principle of sovereignty. Besides the purpose of maintaining international peace and security, this prohibition also influences s State's ability to use armed force against non-State actors in the territory of another State.

**France LOAC Manual**

The French Manual is also of the view that the principles governing the use of force are applicable to the conduct of states in cyberspace. Certain operations, based in its scale and effects can constitute a violation of the prohibition of the use of force; and in this domain, the threshold for the use of force depends not on the digital means used, but on the effects of that cyber operation.

This Manual also agrees that it is not excluded that a cyber operation without physical effects could also be qualified as a use of force, especially considering the origin of that operation, the nature of the instigator, or even the nature of the target[84].

**Denmark LOAC Manual**

The Danish Manual also refers to cyber warfare and use of force; nevertheless, they clarify since the beginning that the Denmark's Computer Network Operations[85] is developing, meaning that this is an area in which the Danish armed forces have still little experience. The manual then explains that the cyber domain is to be subjected to the

[84] For example, the French Manual considers that penetrating military systems to compromise French defence capabilities could be considered a use of force, even if these actions have not yet been followed by its effects.

[85] Computer Network Operations (CNO) is the same as Cyber operations.

existing rules of IL. Additionally, as them being treated as "means of combat (…) there is no separate chapter on CNO"[86].

Regarding the use of force, Chapter 3.7.2. of the Denmark's Manual refers from the beginning, the non-prohibited use of force under the Security's Council authorisation[87]; under the powers conferred by the Security Council, a State may use "all necessary force" or "all necessary means"[88]. Additionally, the Manual mention that "any use of force must be exercised within the framework of other rules of international law"[89].

[86] Military Manual on international law relevant to Danish armed forces in international operations (2016). Para. 3.10. p. 96. Available here: https://www.forsvaret.dk/globalassets/fko---forsvaret/dokumenter/publikationer/-military-manual-updated-2020-2.pdf.

[87] Chapters VI and VII of the U.N.Charter, available here: https://www.un.org/en/about-us/un-charter/full-text.

[88] The Manual provides the example of Resolution 2155 (2014) of the Security Council (27th May 2014), para. 4: "Decides that the mandate of UNMISS shall be as follows, and authorizes UNMISS to use all necessary means (...)". available here: https://digitallibrary.un.org/record/771722.

[89] Military Manual on international law relevant to Danish armed forces in international operations (2016). Chapter. 3.7.2. p. 137.

## Other States positions

Sweden does not have a LOAC Manual, but in its Position Paper on the Application of International Law in Cyberspace[90] agrees with the position of the ICJ and the Tallinn Manual 2.0; the UN Charter stipulates a prohibition of the threat or use of force, but the international community has not yet determined what acts constitute a use of force; a case-by-case assessment needs to be made in order to understand if a certain act enshrines a use of force under IL.

On the other hand, the governmental website of Canada also addresses this question. Given that this State accepts that international law applies to the cyber domain, and, hence, the Charter of the UN, its website refers article 2(4) of the Charter. In addition, it explicitly refers that "cyber activities may amount to such a threat or use of force where the scale and effects are comparable to those from other operations that constitute the use of force at international law."[91] The assessment is to be done on a case-by-case analysis.

Many States have not yet a LOAC Manual of its own, and others have them from the beginning of the century and even from last century, from a time when the cyber capabilities were not developed sufficiently to be a concern that the States would incorporate in these Manuals[92].

Nevertheless, more than 30 States have already made public its opinion regarding this issue. For example, Czech Republic; its national opinion is that article 2(4) is "one of the core provisions"[93] of the Charter of the U.N. and, besides that, a jus cogens[94]. Therefore, the prohibition of the threat or use of force is deliberately general and applies to cyberspace. Moreover, Czech Republic considers that whether a cyber incident violates de prohibition of the mentioned article needs to be appreciated on a "case-by-case basis"; on the other hand, it refers directly to the Tallinn Manual 2.0, and for it factors to access if a conduct amount to an unlawful use of force.

---

[90] Available here: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjurdWO_siEAxUUUaQEHXF1AIQQFnoECBEQAQ&url=https%3A%2F%2Fwww.government.se%2Fcontentassets%2F3c2cb6febd0e4ab0bd542f653283b140%2Fswedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf&usg=AOvVaw0SY3v0c4HINgoHhnBU28Vp&opi=89978449.

[91] "International Law applicable in cyberspace". Available here: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a12.

[92] For example, see the Manuals of Canada or Australia. Available here: https://usnwc.libguides.com/ld.php?content_id=2998098 and here: https://usnwc.libguides.com/ld.php?content_id=11727121.

[93] See the Czech Republic Position Paper on the application of international law in cyberspace (2024).

[94] A peremptory norm of general international law.

The Estonian state, that was the target to a series of cyber-attacks in 2007[95], has also published its national opinion regarding this theme; it says that "States must refrain in their international relations from carrying out cyber operations which, based on their scale and effect, would constitute a threat or use of force"[96]. Even when acting in the cyberspace, States must comply with its obligations of international law, which includes the UN Charter. This position gives some examples of cyber operations that amount to a use of force, as are operations that target critical infrastructures and result in "serious damage, injury or death, or a threat of such an operation"[97].

China's position is much shorter when compared to the ones already analysed; it does not even have a proper chapter to the use of force. Nevertheless, when mentioning the applicability of IL to cyberspace, China makes a brief reference to the principle of the prohibition of the threat or use of force. It reinforces that the application of principles like this is the "cornerstone of the peace, security and stability in cyberspace."[98]

Other State that has a less extended opinion is Iran; despite this, it has a proper chapter to discuss the use of force and armed attacks. The "Armed forces of the Islamic Republic of Iran believe that certainly, those cyber operations resulting in material damage to property and/or persons in the widespread and grave manner (…) constitute use of force."[99].

On the other hand, it is also important to mention the Common position of the African Union that states clearly that "[t]he prohibition on the threat or use of force is a rule of jus cogens" as well as a "fundamental and cardinal" principle of IL. This rule is a key element of the U.N. Charter, and applies in cyberspace "and governs the conduct of States in relation to ICTs in cyberspace."[100]

As we have already seen, Article 2(4) enshrines the key prescription in IL regarding the use of force; furthermore, according to the Tallinn Manual 2.0, there are two exceptions to this prohibition: uses of force authorised by the Security Council under Chapter VII and self-defence pursuant to article 51 of the Charter. The question now is to understand if a cyber-attack can be considered an armed attack under article 51, unleashing the inherent right to self-defence.

[95] During 22 days, Estonia fell under a cyber-attack from Russia; the attack was politically motivated, and has occurred because of the reallocation of a statue from the Sovietic-era in Tallinn.
[96] See the National position of Estonia (2021).
[97] See the National position of Estonia (2021).
[98] See the National position of the People's Republic of China (2021).
[99] See the National position of Iran (2021).
[100] See the Common position of the African Union (2024).

## Armed attack and cyber attacks

### Initial considerations

Article 51 of the UN Charter provides that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."

This article deals with self-defence, which is the precedent condition in the existence of a lawful armed attack[101]. Therefore, it is important for us to distinguish, in the first line, 'armed attack' from 'aggression'[102]. The latter is one of the situations in which the UN Security Council may use its powers, under Chapter VII of the Charter. Therefore, we are already in position to understand that "an act of aggression can constitute an armed attack" but "it may not always do so."[103][104] The main question is to understand when a cyber-attack amounts to an armed attack for the purposes of the UN Charter.

This discrepancy is necessary and intended by the authors of the Charter; uses of force that stay below the minimum limit of an armed attack are not serious enough to justify a response in derogation of the article 2(4) of the UN Charter, which enshrines an important general prohibition.

On the other hand, the restrictive approach of article 51 wants to prevent unnecessary escalation of inter-estate force. Thereby, it puts the common interest of preserving international peace before the individual interest of states to protect its sovereignty. Only in extraordinary cases, the ones with special severity, does the Charter permit the resource to force in self-defence. Nevertheless, although being permitted, the use of force in self-defence is also limited: firstly, by the principles of proportionality and necessity[105]; and secondly, through the obligation of report of the measures taken to the Security Council.

[101] In the Nicaragua Case, the ICJ ruled that the exercise of the right to individual self-defence is "subject to the State concerned having been the victim of an armed attack." See Nicaragua Case (1986). Para. 195.
[102] Is important to notice that even the wording on both articles 2(4) and 51 is different, suggesting a different threshold for "use of force" and "armed attack"
[103] Schmitt, M. N. (2013). Short form citations. In Tallinn Manual on the International Law Applicable to Cyber Warfare (p. 339, para. 2). list, Cambridge: Cambridge University Press.
[104] See the reference to article 3 paragraph g) of the de Definition of Aggression annexed to General Assembly resolution 3314 (XXIX) made in the Nicaragua Case (1986). Para. 195.
[105] Rule 72 of the Tallinn Manual 2.0 ("A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proporcionate"

## The Tallinn Manual 2.0

The Rule 71 of the Tallinn Manual 2.0 states that "A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right to self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects."[106]

Therefore, it is already clear that the IGE agreed that in some cases, cyber operations may be sufficiently grave to warrant being considered armed attacks[107] under the scope of the Charter. This view is consistent with the opinion of the ICJ, that in its Nuclear Weapons Advisory Opinion referred that the choice of means of attack is immaterial to the conclusion of whether an operation qualifies as an armed attack or not. On the other hand, States practice is also consistent with this view; for example, the U.S LOAC Manual states that the "inherent right of self-defense potentially applies against any illegal use of force"[108].

The IGE is of the view that the term 'armed attack' cannot be assimilated with the term 'use of force'[109]. Indeed, not every use of force rises to the level of an armed attack[110]; the scale and effects needed to consider an act as an armed attack are much higher than the threshold of the use of force. Therefore, only in those cases where the use of force reaches the brink of an armed attack, is the state entitled to respond with force in self-defence.

The expression 'scale and effects' was first used in the Nicaragua Case in 1986. The ICJ noted the need to differentiate the most grave forms of the use of force (the ones amounting to an armed attack) from the less grave forms[111]. But that was it. No further guidance was provided in this regard by the Court; the limits of the scale and effects criteria remain unsettled – the effects only need to be considered grave.

---

[106] Schmitt, M. N. (2013). Short form citations. In Tallinn Manual on the International Law Applicable to Cyber Warfare (p. 339). list, Cambridge: Cambridge University Press.

[107] The IGE discussed if the notion of armed attack necessarily involves the use of weapons, and have reached to the conclusion that it did not; the key factor was whether the effects of that cyber operation were analogous to those that would result from an action otherwise qualifying as a kinetic armed attack. Nevertheless, there was an opinion by which the term 'armed' applies exclusively to the use of weapons. in this view, it is mandatory that the cyber operation involves the use of some kind of cyber weapon in order to qualify it as an armed attack.

[108] DoD Manual, p. 1030, para. 16.3.3.1.

[109] Rule 69 of the Tallinn Manual 2.0.

[110] See Nicaragua Case (1986). Para. 191.

[111] Yoram Deinstein has suggested in its "Cyber War and International Law: Concluding Remarks at the 2012 Naval WarCollege International Law Conference, International Law Studies 89" (2013; p. 280) that the gap between 'armed attack' and 'use of force', if it even exists, has been exaggerated by the ICJ over the years, being in reality very restricted. The author actually says that the only cases when a use of force does not reach the threshold of na armed attack, is the cases where that use of force does not result in any victims or destruction of property.

Beyond that, the law is unclear regarding the exact point at which the effects of a certain cyber operation qualify it as an armed attack[112]. Nevertheless, some cases are crystal clear. The Tallinn Manual 2.0 refers that "the International Group of Experts agreed that a cyber operation that seriously injures or kills a number of persons or that causes significant damage to, or destruction of property, would satisfy the scale and effects requirement."[113]

Other important question posed by the Tallinn Manual 2.0 is whether a State can exercise its right to self-defence to a series of cyber-attacks that individually do not rise to the level of an armed attack, but when considered as a whole must be considered. The IGE concluded that the crucial point is whether the attacks have the same originator or originators acting together; if the same perpetrator has carried out small-scale operations that are related and that if aggregated meet the scale and effects requisite, then there are grounds for treating the incident as a composite armed attack[114].

On the other hand, it is also relevant to question which effects are to be considered when assessing if a cyber operation amounts to an armed attack. The IGE unanimously agreed that "all reasonably foreseeable consequences of the cyber operation, so qualify."[115] However, the Group was divided regarding the requisite of intention. Despite this division, the majority is of the view that intention is irrelevant, meaning that only scale and effects matter when qualifying an operation as an armed attack[116].

In the case of bleed-over effects in a third State, most of the Experts agreed that if those effects meet the Scale and Effects threshold for an armed attack, then this third state can also resort to a lawful use of force as self-defence. Even in those cases where the operations against one state do not reach the threshold of an armed attack, if its bleed-over effects do reach the gravity of an armed attack, this third State can defend itself resourcing to force.

It is clear that there are two relevant factors when assessing if a cyber operation amounts to an armed attack: the trans-border and the scale and effects requirements. Nonetheless, it is important to understand that the IGE did not reach consensus on whether

[112] The ICJ in its Nicaragua Case has even distinguished an armed attack from "mere Frontier incident[s]". See Nicaragua Case, para. 195. Nevertheless, many scholars have criticised this view; they adopt the view that only inconsequential actions should be excluded.
[113] Schmitt, M. N. (2013). Short form citations. In Tallinn Manual on the International Law Applicable to Cyber Warfare (p. 342, para. 8). list, Cambridge: Cambridge University Press.
[114] This approach is also known as Pin-prick Theory or the Accumulation Effects Theory.
[115] SCHMITT Michael et al., "Tallinn Manual 2.0", 2nd Ed., Cambridge University Press, Tallinn. 2017. Rule 71, p. 343. Para. 13.
[116] Always comporting with the principle of necessity and proporcionality (Rule 72 of the Tallinn Manual 2.0).

further criteria must be observed to allow a use of force in self-defence. Some are of the opinion that, for example, the intention or the motives are irrelevant, but the agreement of the Experts was that states practice should deal with this matter.

## The LOAC Manuals

### U.S LOAC Manual

The DoD LOAC Manual does not provide any legal criteria to characterise cyber operations as armed attacks. The Manual conclude that any use of force under the scope of article 2(4) "must have a proper legal basis in order not to violate jus ad bellum prohibitions on the resort to force."[117] After this statement, the Manual sends us to Chapter 1, to the general provisions regarding the use of force; it reaffirms the conclusions of Chapter 16, adding that the legality of the use of force needs to be assessed in light of the specific circumstances and facts of the incident.

In a footnote, the north American manual quotes Daniel Webster, that refers lightly a "right of self-defence [that] attaches always to nations as well as to individuals". Despite not mentioning the inherent right of self-defence present in article 51 of the Charter, the mere fact that the DoD is quoting a scholar that refers to this right, makes it understandable that the position of the Manual is the same as the Tallinn Manual 2.0.

Furthermore, there are other chapters of this LOAC Manual where the authors refer explicitly to the right of self-defence; in Chapter 1.11.1.2., the Manual literally states that "force can be used in self-defence, but only to the extent that it is required to repel the armed attack and to restore the security of the party attacked."[118]

### Spain LOAC Manual

On the other hand, the Spanish LOAC Manual is much clearer in this matter. Chapter 4.3.3. refer to Chapter 1.1.1. and 1.2.2.2 but has also some notes regarding this matter in this Chapter dedicated to cyber operations.

This Manual expressly recognises article 51 of the UN Charter as an instrument of IL that gives the States legitimacy to act in self-defence. Additionally, it states that the resource to force in self-defence must be preceded by an armed attack. Likewise, the Manual affirms that a kinetic response in self-defence can be used against a cyber-attack, always responding with respect for the principles of necessity and proportionality[119].

Spain's LOAC Manual refers that, to qualify a cyber incident as an armed attack, there are two important conditions: firstly, the cyber operation needs to have a cross border

[117] DoD Manual, p. 1039, para. 16.3.1.
[118] DoD Manual, p. 41, para. 1.11.1.2.
[119] "Una respuesta cinética en legítima defensa contra un ciberataque puede ser legal si es necesaria para poner fin al ataque y responder proporcionalmente en atención al método e impacto de la agresión." "Derecho Internacional humanitario (DIH) em las FAS". P. 113, par. 0441.

character[120], which is fulfilled when a state takes part in a cyber operation that would be considered an armed attack, if was a kinetic operation. Moreover, this cross-border nature also exists if the perpetrator State had ordered non-State actors to act in its behalf, no matter where they were.

On the other hand, to be considered an armed attack, the operation should have effects that reach a certain level of severity[121]. Nevertheless, the Manual does not go further in this matter, and does not enlighten regarding the concrete level of severity needed to reach the armed attack threshold[122].

The Spanish LOAC Manual, notwithstanding not specifying the concrete level of severity, refers three theories regarding the definition of armed attack. Firstly, the theory of nature through which the attack produces necessarily damage or destruction in objects or injury or death to people. Secondly, the theory of effects, which provides that the extension of the effects of the attack are much relevant. Lastly, the theory of the physical objective according to which the attack must be directed to critical infrastructures, causing severe effects in them.

Besides this, the Manual also refers to necessity and proportionality as requirements for the resource to self-defence. The requirement of necessity is fulfilled when the resort to non-coercive measures is not enough to stop the attack. On the other hand, proportionality concerns the scale, reach, length, and intensity of the defensive response.

**Norway LOAC Manual**

The Norwegian LOAC Manual refers that the prohibition against the use of force and against intervention are two principles which the fundamental purpose is to maintain international peace and security. Furthermore, it mentions three exceptions from the prohibition of the use of force against other states: firstly, the UN mandate, that is, from the Security Council under Chapter VII. For that, the Security Council must decide that a situation exists that threatens international peace and security in such way that is necessary the use of armed force.

[120] "tiene que traspasar los límites propios de un Estado, es decir, ha de poseer un carácter transfronterizo." "Derecho Internacional humanitario (DIH) em las FAS". P. 113, par. 0443.
[121] The Manual refers to the Nicaragua Case, quoting the ICJ when it says that armed attacks are the "most grave" forms of use of force.
[122] This LOAC Manual allows preemptive self-defence in those cases in which the threat of use of force is instantaneous and overwhelming, and when there is no time to deliberate; the threat is imminent.

Other exception present in the Manual is the right to self-defence of the States. "An armed attack on a state gives that state the right to act in self-defence in accordance with international law"[123], namely under article 51 of the Charter[124].

In Norway, it is "up to the government to evaluate and determine whether Norway is subject to an armed attack such that [it] may act in self-defence in accordance with international law."[125]

These provisions are general, but also apply to the cyber context, given the fact that the Manual states clearly that "[c]yberattacks are subject to the same restrictions and regulations as other types of attacks."[126]

**France LOAC Manual**

The French Manual states that certain cyber operations, based on its scale and effects, can constitute a violation of the prohibition of the use of force of the Article 2(4) of the Charter of the UN The Manual then clarifies that in the digital space, the threshold for the use of force depends not on the digital means used, but on the effects of the cyber operation.

When the effects of a cyber-attack are similar to those resulting from the use of a conventional kinetic weapon, then that cyber incident may constitute a violation of the prohibition of the use of force. Therefore, it is also important to enhance that cyber operations that do not produce physical effects can also be qualified as uses of force, especially considering the origin of the operation, the nature of the instigator, the intended effects, or the nature of the target[127].

An armed aggression is a use of force of significant gravity, regardless of the means used. Therefore, it is not excluded that a cyber incident may constitute an armed attack within the meaning of article 51 of the UN Charter, when its scale and effects reach a certain gravity and are comparable to those of physical force.

The French LOAC Manual concludes that to be considered an armed attack, a cyber operation must also have been perpetrated, directly or indirectly, by a State. Apart from acts committed by individuals belonging to state organs or exercising public authority, a

[123] Chapter 51 of the Charter of the U.N.

[124] This article provides na independente basis for the use of force; nevertheless, this use of force is conditional upon immediate reporting to the Security Council, being valid only until the Security Council implements, itself, measures to ensure international peace and security.

[125] Manual of the Law of Armed Conflict (2013). P.9, para. 1.10. Available here: https://usnwc.libguides.com/ld.php?content_id=47416967.

[126] Manual of the Law of Armed Conflict (2013). P. 209, para. 9.53.

[127] E.g. penetrating military systems to compromisse French defence capabilities could be considered a use of force, even if those actions have not yet been followed by its effects.

State is responsible for acts committed by non-State actors only if the latter have acted on the first instructions or under its control.

France's LOAC Manual refers to countermeasures as a way of responding to state-sponsored cyber-attacks. This may pose a problem, given that attribution is a complex problem in cyberspace. However, the Manual provides that States can take retaliatory measures, which may include, among others, making public protests, suspending agreements, or activating diplomatic initiatives[128].

These countermeasures[129] must be carried out in compliance with certain obligations of international law, such as the prohibition of resorting to the threat or use of force or obligations concerning the protection of fundamental human rights.

According to this Manual, an armed aggression gives the victim State the right to exercise individual or collective self-defence. This is the only unilateral recourse to armed force that is lawful. Self-defence in response to an armed aggression conducted in cyberspace can be implemented through means in the physical or digital realms, respecting the principles of necessity and proportionality.

In exceptional circumstances, it is possible to resort to preemptive self-defence in response to a cyber-attack "not yet initiated but about to be, in an imminent and certain manner, provided that the potential impact of this aggression is sufficiently serious."[130] [131]

The possibility of a response demand that the cyber operation is characterized as reaching a certain threshold of severity, and that threshold is determined on a case-by-case analysis.

France has established its doctrine to identify cyber operations that may amount to an armed attack under article 51 of the Charter; it is a scale of severity that has six levels[132]. Notwithstanding having those levels, the last one is the only that may enshrine an armed

[128] "Le droit international est applicable aux cyberopérations". Chapter 4. P. 303-304. Manuel de droit des opérations militaires (2022).
[129] Article 49 of the Draft Articles on the Responsibility of States for Internationally Wrongful Acts and jurisprudence recognize the right to use countermeasures solely to the aggrieved state.
[130] « non encore déclenchée, mais sur le point de l'être, de façon imminente et certaine, pourvu que l'impact potentiel de cette agression soit suffisamment grave ». SGDSN, Revue stratégique de cyberdefense (2018). p. 84.
[131] Just like in the physical realm, preventive self-defence is not recognized by international law and cannot be implemented in cyberspace.
[132] The first level being Level 0, with a insignificant impact ("impact négligeable"); Level 1A, with low impact ("impact faible"); Level 1B with significant and circunscrite impact ("impact significatif et circonscrit"); Level 2, with strong and circunscrite impact ("impact forte t circonscrit"); Level 3, with strong and extended impact ("impact fort et étendu"); Level 4, with major impact ("impact majeur"); and lastly, Level 5, with extreme impact ("impact extreme").

attack under article 51. It is probably impossible to characterise all the others five levels as an armed attack [133].

**Denmark LOAC Manual**

The Danish LOAC Manual also refers to article 51 of the Charter. However, it considers that the right to self-defence is not an inherent right under the Charter, but "is recognised in customary international law."[134] On the other hand, this Manual states that the attack being perpetrated by a non-State actor has no effect in the right to self-defence of the aggressed State.

The Denmark's Manual also mentions two requisites of the act of self-defence. First, it that act must be necessary to "prevent or suspend the attack or new attacks that are assessed to follow"[135]. Moreover, it also needs to be proportional, meaning that a proportionality teste needs to be done "between the act of attack and the act of self-defence"[136].

Regarding cyber operations, the manual is also very clear: cyber-attacks[137] against or in Denmark, even though possibly having consequences that can be equated with more conventional armed attacks, "the initiator of the attack must be identifiable as a prerequisite for a legitimate act of self-defence."[138]

[133] See chart present in page 306 of the French LOAC Manual.
[134] Military Manual on International Law relevant to Danish armed forces in international operations (2016). P. 36. Available here: https://usnwc.libguides.com/ld.php?content_id=59166472.
[135] Military Manual on International Law relevant to Danish armed forces in international operations (2016). P. 36.
[136] Military Manual on International Law relevant to Danish armed forces in international operations (2016). P. 37.
[137] Referred as CNA – computer network attacks.
[138] Military Manual on International Law relevant to Danish armed forces in international operations (2016). P. 37.

**Other States positions**

Czech Republic has made its official opinion public in 2024. It states that "depending on the facts and circumstances, cyber operations (…) may also constitute an "armed attack", under Article 51 of the UN Charter."[139] The State's position affirms that despite the UN Charter not giving a definition for the term "armed attack" nor listing the criteria for determining what conditions are needed to consider an act as a armed attack, the position to be followed is the one provided by the ICJ: the relevant factors are the scale and effects of the particular act.

On the other hand, "[t]he Czech Republic reiterates the provisions of the UN Charter and customary international law that if an armed attack occurs, the affected State may exercise its inherent right to individual or collective self-defence under Article 51 of the UN Charter."[140]

The Republic of Estonia also agrees with this view and accepts the criteria of scale and effects when assessing whether an operation amounts to an armed attack. If the effects of a cyber incident are similar or equivalent to a kinetic attack, then it could constitute an armed attack, which triggers the right to self-defence present in the Charter, with all its limits, such as proportionality and necessity.

At the same time, Estonia refers that the attacked State is not "necessarily limited to taking measures by cyber means"[141]; all means are available for the State to defend itself, as long as in a proportionate way and according with the provisions of IL.

China's position is narrower. With only six chapters, it does not refer to armed attacks nor to the right to self-defence of States. The same with the National position of the Russian Federation, with zero references to armed attacks or the right to self-defence.

By the contrary, Iran believes that the right to self-defence should be reserved "if the gravity of the cyber operation against the vital infrastructure of the state is reached in the threshold of the conventionally armed attack"[142]

The Common position of the African Union is much more detailed. It mentions two exceptions to the prohibition of the use of force, being one of them the right of self-defence when an armed attack occurs. "In particular, a cyber operation, depending on its scale and effect, would amount to use of force if it is expected to cause physical damage, injury, or

[139] See the Czech Republic Position Paper on the application of international law in cyberspace (2024).
[140] See the Czech Republic Position Paper on the application of international law in cyberspace (2024).
[141] See the National position of Estonia (2021).
[142] See the National position of Iran (2020).

death, that is comparable to the use of force by an act covered by the prohibition."[143] The criteria to understand whether we're facing a use of armed force is the scale and effects of the operation.

The African Union distinguish between the gravest forms of the use of force, which constitute an armed attack allowing the States to respond under the right to self-defence, and the less grave forms of the use of force. This needs to be asserted on a case-by-case analysis, and taking into account different criteria such as "the duration of the attack, the nature of the targets attacked, the locations of the targets attacked, and the types of weapons used"[144]. Furthermore, the Common opinion also refers that the right to self-defence can only be triggered when an armed attack is attributable to a State.

On the other side, Canada's governmental website "considers that the inherent right of self-defence if an armed attack occurs against a State also applies in cyberspace."[145] Canada will respond to cyber activities that reach the threshold of an armed attack in a manner that is consistent with the international law and, namely, the U.N. Charter. Therefore, that response may or may not include cyber activities.

Other country that does not have a LOAC Manual, but has also something to say in this regard, is Sweden. In its Position Paper on the Application of International Law in Cyberspace[146], Sweden recognises a right to self-defence when an armed attack occurs. In addition, it is not a requisite that the attack uses kinetic means; in the same way, it is not also a requirement that the response to that attack use kinetic means.

Therefore, a cyber-attack may rise to the level of an armed attack when its scale and effects are comparable to a kinetic armed attack. In those cases, the exercise of self-defence must be immediately communicated to the Security Council of the U.N. Moreover, the exercise of self-defence needs to be articulated with the fundamental principles of necessity and proportionality.

[143] See the Common position of the African Union (2024), para 39.
[144] See the Common position of the African Union (2024), para. 41.
[145] "International Law applicable in cyberspace" (2022). Available here: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a12.
[146] Available here: https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf.

Why do States do not apply article 51 to cyber incidents?

As already seen, the opinio juris is that article 51 of the UN Charter do apply to the cyber domain. Therefore, theoretically, there may have already been cases of cyber-attacks that rise to the level of armed attacks, triggering the right to self-defence of states.

Indeed, the Center for Stategic & International Studies has launched a list of cyber incidents, dating from early 2006 up until January of 2024. This timeline counts with more than 90 pages of incidents.

According to the Council on Foreign Relations[147], China has sponsored over 240 cyber operations, followed by Russia with 195 sponsored cyber operations, and Iran, with 94 sponsored operations. These are the top three countries regarding the founding of cyber operations[148].

Let's look at Stuxnet, for an instance. Stuxnet is considered by some as the first cyberweapon ever to exist[149]. It was described, among other things, as the first malicious software (malware) designed specifically to attack a particular type of industrial control system[150]. Stuxnet is a computer virus that caused the destruction of over 1,000 centrifuges in Natanz, Iran, and that is attributed to Israel and U.S. joint operation 'Olympic Games'. The authors of the worm could spy and control the industrial systems, leading to the fast spinning of the centrifuges, that tear themselves apart unbeknownst to the human operators at the plant.

Therefore, we can already understand that Stuxnet had quite an impact in Iran's Nuclear Program. As said before, it has destroyed many nuclear centrifuges, causing millions of dollars of damages for Iran.

The whole world saw the Olympic Games Operation accomplish, at least in part, its goals, delaying the development of a new nuclear world power. The question that remains is: why did no one talk about an armed attack? Did this cyber operation not reach the threshold of an armed attack?

Looking at the States position, it is clear that the scale and effects of the incident was high enough to fall, at least, within the scope of article 2(4), and who knows, even in the

[147] An independent and nonpartisan organisation, think tank and publisher whose gole is to being a resource to its members, governments, journalists civic and religious leaders, etc., to help them understand the foreign policy choices facing the United States and other countries.
[148] Between 2005 and 2023.
[149] "Cyberwarfare and Cyberterrorism: In Brief" (2015). P. 1. Available here: https://sgp.fas.org/crs/natsec/R43955.pdf.
[150] "Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme" (2020). P. 66. Available here: https://securityanddefence.pl/pdf-121974-52879?filename=Operation%20_Olympic.pdf.

scope of article 51, triggering the right to self-defence of Iran. But the truth is that no one, not even the Iranian State, talked about an armed attack.

Other important example is the Estonia case. As previously mentioned, Estonia suffered a major cyber-attack from Russia, back in 2007. The operation had political motivations and was perpetrated by Russia[151].

Estonia was hit by these major DDoS cyber-attacks which lasted weeks. From media outlets to government bodies, many services were taken down in this unprecedented attack. Day-to-day life was very affected since cash machines and online banks were out of action, as well as small businesses. Government employees could not work nor use their emails. Newspapers and broadcasters could not deliver the news. Moreover, it exposed Estonia's vulnerabilities, illustrating the potential of cyber-attacks to cause long lasting effects.

More recently, during the conflict between Russia and Ukraine, the international community acknowledge that Russia has been attacking Ukraine by cyber means repeatedly. But, again, no one has dared to refer to armed attack.

The fact that hundreds of cyber incidents have been happening in the last decade, and no references exist regarding a possible armed attack, make us think that, in the cyber domain, article 51 of the Charter is devoid of useful meaning – is empty.

As we saw, the Tallinn Manual 2.0 is very clear when assuming 'Scale and Effects' as the paramount criteria when assessing whether a cyber-attack amounts to an armed attack. And if up until the beginning of 2024, this position was accepted and recognized by NATO countries and a few more western countries, the truth is that with the Common position of the African Union, this position acquired a whole new universal dimension.

We are now in the position of saying that this is the positioning of the international community. Nevertheless, it remains unsettled why the States don't follow their own opinions and LOAC Manuals; why they keep on accepting repeated cyber-attacks, with major impact in the life of its citizens. The UN Charter opens a door for self-defence and States are not using it to protect its national interests.

[151] The malicious traffic clearly contained Russian language background. On the other hand, instructions to attack Estonia were spread in Russian websites and forums. Despite Russia always denied being the perpetrator of the attacks, a well known russian hacker Sp0Raw believes that the attacks could not have been executed without the consent of the Russian authorities.

Some may say that States are not using article 51 of the Charter given the problem of attribution. Attribution is considered by many as "one of the most intractable problems"[152] of the fifth domain.

But it's clear that attribution is an inevitable portion of the cyber domain. Being incredibly scattered, this field of operations is in constant development, changing day by day. The fact that in most of cases it is impossible to find the real perpetrator is inherent to this domain.

Being decentralized as it is, with the possibility of one person leading a cyber operation in one part of the world that is going to affect States in the opposite side, attribution is the cyber domain birth right, which should not be an excuse for States to not apply article 51, and protect its national superior interests.

[152] Thomas Rid & Ben Buchanan (2015) Attributing Cyber Attacks, Journal of Strategic Studies. P. 5. Available here: https://cs.brown.edu/courses/cs180/sources/Attributing_Cyber_Attacks.pdf.

## Conclusion

This paperwork objective was to understand and compare States positions regarding the problem of application of articles 2(4) and 51 of the UN Charter to cyber operations. The conclusion reached is that these articles do apply to the cyber domain, with all its consequences and restrictions.

Nevertheless, it is also possible to conclude that the national positions of States are not reflecting its practices in the real world. Today more than ever, the humanity is facing dark days, with many points of tension around the world; crisis are arising in all continent, and this new domain fulfils an important role in today's warfare.

Despite the increasing relevance of ICTs, States continue to not resort to its right to self-defence, in the light of article 51 of the Charter. Either for being too afraid of the consequences, or because they have full knowledge of them, States are refraining of call 'armed attack' to any cyber operations, regardless its scale and effects, that in some circumstances are severe enough to, in theory, fall within the scope of the mentioned article.

## References


*2007 cyber attacks on Estonia*. (2013). Retrieved from NATO Strategic Communications Centre of Excellence: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf , last visited on the 19th January 2024

*71 UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security.* (2017, June). Retrieved from Representaciones Diplomáticas de Cuba en el Exterior: http://misiones.cubaminrex.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information , ast visited on the 18th February 2024

Alvarez, J. (2015, february 03). *Stuxnet: The world's first cyber weapon* . Retrieved from Stanford University: Center for International Security and Cooperation : https://cisac.fsi.stanford.edu/news/stuxnet , last visited on the 19th January 2024

Armées, M. d. (2022). *Manuel de droit des opérations militaires.* (C. Faure, Ed.) Retrieved from Ministère des Armées: https://www.defense.gouv.fr/sites/default/files/sga/Manuel%20de%20droit%20des%20opérations%20militaires_édition%202022.pdf , last visited on the 1st of April 2024

Assembly, G. (2014, January). *Resolution adopted by the General Assembly on 27 December 2013 [on the report of the First Committee (A/68/406)] .* Retrieved from United Nations: https://documents.un.org/doc/undoc/gen/n13/454/03/pdf/n1345403.pdf?token=XK458rNomMpZ9v0Yw9&fe=true , last visited on the 3rd of March 2024.

Assembly, G. (2015, December). *Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455)] .* Retrieved from United Nations: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf , last visited on the 5th of January 2024.

Assembly, G. (2021, December). *Resolution adopted by the General Assembly on 6 December 2021 [on the report of the First Committee (A/76/439, para. 7)].* Retrieved from United Nations: https://documents.un.org/doc/undoc/gen/n21/377/48/pdf/n2137748.pdf?token=5CnM9k23DNmVSnJ8To&fe=true , last visited on the 5th of January 2024.

Birth of telephone. (1899, july 09). *Omaha Daily Bee*, p. p. 6. Retrieved from Library of Congress: https://guides.loc.gov/chronicling-america-telephone-invention , last visited on the 6th of December 2023.

Buchan, R., & Tsagourias, N. (2024, February 20). *The African Union's Statement on the Application of International Law to Cyberspace: An Assessment of the Principles of Territorial Sovereignty, Non-Intervention, and Non-Use of Force*. Retrieved from EJIL: Talk!: https://www.ejiltalk.org/the-african-unions-statement-on-the-application-of-international-law-to-cyberspace-an-assessment-of-the-principles-of-territorial-sovereignty-non-intervention-and-non-use-of-force/ , last visited on the 8th of March 2024.

Buchanan, T. R. (2015). *Attributing Cyber Attacks*. Retrieved from Journal of Strategic Studies: https://cs.brown.edu/courses/cs180/sources/Attributing_Cyber_Attacks.pdf , last visited on the 19th of January 2024.

Canada, G. o. (2022, April). *International Law applicable in cyberspace*. Retrieved from Government of Canada: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a2

CloudFlare. (2024). *What is a DDoS attack?* Retrieved from CloudFlare: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ , last visited on the 6th December 2023.

CloudFlare. (2024). *What is a denial-of-service attack?* Retrieved from CloudFlare: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/ , last visited on the 6th December 2023.

College, N. D. (2013). *Manual of the Law of Armed Conflict* (First ed.). (T. C. Defence, Ed.)

Comission, E. (2020, December). *The EU's Cybersecurity Strategy for the Digital Decade.* Retrieved from European Comission: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjk_9agtsmEAxWe_rsIHa0SB9IQFnoECB4QAQ&url=https%3A%2F%2Fdigital-strategy.ec.europa.eu%2Fen%2Flibrary%2Feus-cybersecurity-strategy-digital-decade-0&usg=AOvVaw1dPdwYw0N1 , last visited on the 3rd January 2024.

Commission, I. L. (2001). *Responsability of States for Internationally Wrongful Acts.* Retrieved from United Nations: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf , last visited on the 2nd of April 2024.

Council, N. R. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington D.C.: National Academy Press , last visited on the 28th of March 2024.

Cross, I. C. (1949). *The Geneva Conventions of 12 August 1949.* Retrieved from International Committee of the Red Cross: https://www.icrc.org/en/doc/assets/files/publications/icrc-002-0173.pdf , last visited on the 2nd of December 2023.

Cross, I. C. (2024). *Distinction*. Retrieved from IRCR.ORG: https://casebook.icrc.org/a_to_z/glossary/distinction , last visited on the 2nd of April 2024.

*Código Penal Português* (9.ª ed.). (1982). Almedina , last used on the 2nd of December 2023.

*CYBERSECURITY HISTORY: HACKING & DATA BREACHES*. (2024). Retrieved from Monroe College: https://www.monroecollege.edu/news/cybersecurity-history-hacking-data-breaches , last visited on the 2nd of April 2024.

*cyberspace operations (CO)*. (2024). Retrieved from Information Technology Laboratory COMPUTER SECURITY RESOURCE CENTER: https://csrc.nist.gov/glossary/term/cyberspace_operations , last visited on the 2nd of April 2024.

Defence, D. M. (2020). *Military Manual on International Law relevant to Danish armed forces in international operations.* Retrieved from Danish Ministry of Defence: https://www.forsvaret.dk/globalassets/fko---forsvaret/dokumenter/publikationer/-military-manual-updated-2020-2.pdf , last visited on the 4th of April 2024.

Defence, M. o. (2012). *The Defence Cyber Strategy.* Retrieved from Minestry of Defence: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Netherlands_2012_NDL-Cyber_StrategyEng.pdf , last visited on the 8th of March 2024.

Defence, M. o. (2015). *Department of Defense Law of War Manual.* United States of America , last visited on the 4th of April 2024.

Defence, M. o. (2022). *Cyber Primer* (Third ed.) , last visited on the 5th of April 2024.

Defence, M. o. (2022). *Derecho internacional humanitario (DIH) en las FAS ,* last visited on the 5th of April 2024.

Defence, O. o. (2023, july). *Department of Defense Law of War Manual.* Retrieved from U.S. Department of Defense: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwil2PTUip6EAxUPgP0HHQmrAMUQFnoECBoQAQ&url=https%3A%2F%2Fmedia.defense.gov%2F2023%2FJul%2F31%2F2003271432%2F-1%2F-1%2F0%2FDOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%2 , last visited on the 5th of April 2024.

*EU Statement – United Nations 1st Committee: Thematic Discussion on Other Disarmament Measures and International Security.* (2018, october). Retrieved from European Union - External Action: https://www.eeas.europa.eu/node/52894_en , last visited on the 15th March 2024.

Faure, C. (Ed.). (2022). *Manuel de droit des opérations militaires ,* last visited on the 1st of April 2024.

Foltz, A. C. (2012). Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate. *Joint Force Quarterly (JFQ)* , last visited on the 13th March 2024.

Force, N. Z. (2019). *Manual of Armed Forces Law.* Retrieved from New Zealand Defence Force: https://usnwc.libguides.com/ld.php?content_id=47364407 last visited on the 1st of April 2024.

G20. (2015, november). *G20 Leaders' Communiqué Antalya Summit.* Retrieved from Atalaya Summit: https://www.gpfi.org/sites/gpfi/files/documents/G20-Antalya-Leaders-Summit-Communiqu--.pdf , last visited on the 19th March 2024.

GGE. (2013, June). *2013 UN GGE Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/68/98).* Retrieved from United Nations: https://dig.watch/wp-content/uploads/A_68_98_E.pdf , last visited on the 13th March 2024.

GGE. (2015, July). *2015 UN GGE – Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/70/174).* Retrieved from United Nations: https://undocs.org/A/70/174 , last visited on the 13th March 2024.

GGE. (2021, July). *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security - 2015.*

Retrieved from United Nations: https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf , last visited on the 24th of February 2024.

Gordon, E. (n.d.). *Article 2(4) in Historical Context.* Retrieved from Core.uk: https://core.ac.uk/download/pdf/72839491.pdf , last visited on the 30th of March 2024.

Gray, C. (2018). *International Law and the Use of Force.* Oxford: Oxford University Press. , last visited on the 28th of March 2024.

Helal, M. (2024, February 2). *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, and all associated Communiqués adopted by the Peace and Security Council of the African Union.* Retrieved from EJIL: Talk!: https://www.ejiltalk.org/the-common-african-position-on-the-application-of-international-law-in-cyberspace-reflections-on-a-collaborative-lawmaking-process/ , last visited on the 1st of April 2024

Jackson, P., & Gerken, T. (2024, january 30). *Elon Musk says Neuralink implanted wireless brain chip*. Retrieved from BBC News: https://www.bbc.com/news/technology-68137046 , last visited on the 3rd of February 2024.

Jensen, E. T. (2017). *The Tallinn Manual 2.0: highlights and insights.* Retrieved from Geogetown Journal of International Law: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/07/The-Tallinn-Manual-2.0-article_compressed.pdf , last visited on the 12th of January 2024.

Justice, I. C. (1996, July 8). *Reports of judgments, advisory opinions and orders legality of the threat or use of nuclear weapons.* Retrieved from International Court of Justice: https://www.icj-cij.org/sites/default/files/case-related/95/095-19960708-ADV-01-00-EN.pdf , last visited on the 16th January 2024.

Kamiński, M. A. (2020). *Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme.* Retrieved from securityandefence: https://securityanddefence.pl/pdf-121974-52879?filename=Operation%20_Olympic.pdf , last visited on the 28th of March 2024.

Kuru, H. (2017, February). Prohibition of Use of Force and Cyber Operations as "Force". *Journal of Learning and Teaching in Digital Age*, pp. 46-53. , last visited on the 16th of January 2024

Kushner, D. (2013, February 26). *The real story of Stuxnet*. Retrieved from IEEE Spectrum: https://spectrum.ieee.org/the-real-story-of-stuxnet , last visited on the 28th of february 2024.

*Ley Orgánica 14/2015, de 14 de octubre, del Código Penal Militar.* (2015, 10 15). Retrieved from Agencia Estatal Boletín Oficial del Estado: https://www.boe.es/buscar/act.php?id=BOE-A-2015-11070 , last visited on the 19th of December 2024.

McAfee. (2021, july 30). *O que é um vírus trojan e como remover*. Retrieved from McAfee: https://www.mcafee.com/blogs/pt-pt/internet-security/compreender-os-virus-troianos-e-como-se-livrar-deles/ , last visited on the 12th december 2024.

McGuinness, D. (2017, april 27). *How a cyber attack transformed Estonia*. Retrieved from BBC News: https://www.bbc.com/news/39655415 , last visited on the 4th of January 2024.

Ministros, C. d. (2022, November 2). *Resolução do Conselho de Ministros n.º 106/2022.* Retrieved from Diário da República: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi047-14e6EAxW8RaQEHdOzAjkQFnoECA8QAQ&url=https%3A%2F%2Fdiariodarepublica.pt%2Fdr%2Fdetalhe%2Fresolucao-conselho-ministros%2F106-2022-202899924&usg=AOvVaw1OebKoH4ja3Mo , last visited on the 23rd of February 2024.

Nations, U. (1977, June 8). *PROTOCOL ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, AND RELATING TO THE PROTECTION OF VICTIMS OF INTERNATIONAL ARMED CONFLICTS (PROTOCOL I), OF 8 JUNE 1977 .* Retrieved from United Nations: https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.34_AP-I-EN.pdf , last visited on the 27th of March 2024.

OAS. (2020). *AG/RES. 2959 (L-O/20).* Retrieved from Organisation of American States (OAS): http://www.oas.org/en/sla/iajc/docs/AG-RES_2959_EN.pdf , last visited on the 6th of December 2023

Obama, B. (2011, May). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.* Retrieved from White House: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf , last visited on the 28th of March 2024.

O'Connell, M. E. (2013). *The prohibition of the Use of Force.* Retrieved from Notre Dame Law School: https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1061&=&context=book_chapters&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.pt%252Fscholar%253Fhl%253Dpt-PT%2526as_sdt%253D0%25252C5%2526q%253Dexceptions%252Bto%252Bthe%252Bprohibition%2 , last visited on the 12th of January of 2024.

Ottis, R. (2018). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Retrieved from Cooperative Cyber Defence Centre of Excellence: https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf , last visited on the 3rd of December 2023.

Ottis, R. (2024). *Rain Ottis*. Retrieved from LinkedIn: https://ee.linkedin.com/in/rainottis , last visited on the 10th of April 2024.

Ottis, R. (n.d.). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Retrieved from CCDCOE.ORG: https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf , last visited on the 1st of april 2024.

Rølsåsen. (2016). *When do cyber operations amount to use of force and armed attack, and what response will they justify?* Retrieved from University of Oslo: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwixiI3l7M2EAxWw7rsIHWHRCSoQFnoECBkQAQ&url=ht

tps%3A%2F%2Fwww.duo.uio.no%2Fbitstream%2Fhandle%2F10852%2F50840%2F723.pdf%3Fsequence%3D1&usg=AOvVaw1-qCHjXlkEEHU-ALKTthWG&o , last visited on the 19th january 2024.

Ronzitti, N. (2002). *The current status of the principle prohibiting the use of force and legal justifications of the use of force.* Retrieved from Istituto Affari Internazionali: https://www.iai.it/sites/default/files/iai0215.pdf , last visited on the 17th of march of 2024.

Roosevelt, F. D., & Churchill, W. S. (1941, August). *The Atlantic Charter.* Retrieved from Yale Law School: https://avalon.law.yale.edu/wwii/atlantic.asp , last visited on the 5th of January 2024.

Sari, A. (2023, March 24). *International Law and Cyber Operations: Current Trends and Developments.* Retrieved from Council of Europe: https://rm.coe.int/64th-cahdi-pr-aurel-sari-presentation/1680aaaf48 , last visited on the 25th of March 2024.

Schmitt, M. N. (2010). *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts.* Retrieved from Proceedings of a Workshop on Deterring CyberAttacks: https://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_059439.pdf , last visited on the 30th of March 2024.

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0* (Second ed.). Tallinn: Cambrige University Press. , last visited on the 30th of March 2024.

Stauffacher, D. D. (2019, May). *"UN GGE and UN OEWG: How to live with two concurrent UN Cybersecurity processes".* Retrieved from ICT4Peace.org: https://ict4peace.org/wp-content/uploads/2019/11/ICT4Peace-2019-OEWG-UN-GGE-How-to-live-with-two-UN-processes.pdf , last visited on the 24th of February 2024.

Sweden, G. O. (2022, July). *Position Paper on the Application of International Law in Cyberspace.* Retrieved from Government Offices of Sweden: https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf , last visited on the 1st of April 2024.

*The UN in General.* (n.d.). Retrieved from United Nations: https://unis.unvienna.org/unis/en/topics/the-un-in-general.html , last visited on the 12th March 2024.

Theohary, C. A., & Rollins, J. W. (2015, March). *Cyberwarfare and Cyberterrorism: In Brief.* Retrieved from Congressional Research Service: https://sgp.fas.org/crs/natsec/R43955.pdf , last visited on the 13th March 2024.

*Warsaw Summit Communiqué.* (2016, july 01). Retrieved from North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/official_texts_133169.htm , last visited on the 28th March 2024.