Cadernos do IUM

MILITARY OPERATIONS IN CYBERSPACE

Coordinator:
Lieutenant-colonel João Paulo Ferreira Lourenço

IUM

Abril 2024

INSTITUTO UNIVERSITÁRIO MILITAR

MILITARY OPERATIONS IN CYBERSPACE

Coordinator

Lieutenant-colonel João Paulo Ferreira Lourenço

IUM – Centro de Investigação e Desenvolvimento (CIDIUM)
Abril de 2024

Como citar esta publicação:

Lourenço, J. P. F. (Coord.), (2024). *Military Operations in Cyberspace*. Cadernos do IUM, 59. Lisboa: Instituto Universitário Militar.

Diretor
Tenente-General Hermínio Teodoro Maio

Editora-chefe
Coronel Joana Isabel Azevedo do Carmo Canhoto Brás

Coordenadora Editorial
Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

Capa – Composição Gráfica
Tenente-coronel Ana Carina da Costa e Silva Martins Esteves
Imagem gerada por Inteligência Artificial em abril de 2024

Secretariado
Assistente Técnica Gisela Cristina da Rocha Basílio

Propriedade e Edição
Instituto Universitário Militar
Rua de Pedrouços, 1449-027 Lisboa
Tel.: (+351) 213 002 100
Fax: (+351) 213 002 162
E-mail: cidium@ium.pt
https://cidium.ium.pt/site/index.php/pt/publicacoes/as-colecoes

Paginação, Pré-Impressão e Acabamento
What Colour Is This?
Rua Roy Campbell Lt 5 -4º B
1300-504 Lisboa
Tel.: (+351) 219 267 950
www.wcit.pt

ISBN: 978-989-35731-1-2
ISSN: 2183-2129
Depósito Legal:
Tiragem: 90 exemplares

Nota do Editor:

Os textos/conteúdos do presente volume são da exclusiva responsabilidade dos seus autores.

EDITOR'S NOTE

Dear readers,

I present to you the 59th issue of the "Cadernos do IUM" editorial line, consisting of three texts that offer reflections and studies by researchers from the IUM and its national and international partners, in a comprehensive and up-to-date view of the challenges of international law in cyberspace and its practical application.

The first text addresses the evolution of international law in cyberspace since the 1990s, highlighting important events and milestones, such as the creation of the Tallinn Manual, which has become a global reference. The Tallinn Manual 3.0, under development, is highlighted as a crucial piece to address fundamental issues such as sovereignty and the use of force.

The second text focuses on the challenges of applying international law to cyber operations, from the difficulty of equating cyber attacks with armed attacks to the question of imminence in international law. The attribution in cyber operations and the complexity of the legal response are discussed in detail.

Finally, the third text highlights the crucial role of international support in cyberspace for Ukraine, which redefines war and geopolitics. The expectation regarding Tallinn Manual 3.0 and the importance of considering technological developments and the real technological developments and the actual practices of states are key points in this context.

We hope that these texts will offer a deeper and more up-to-date understanding of a subject as complex and constantly evolving as international law in cyberspace.

Enjoy your reading!

Ana Esteves
Lieutenant-colonel
Editorial coordinator of CIDIUM

INDEX

PREFACE

Professor Michael Schmitt is a renowned international law scholar and was one of the pioneers in publishing studies on the interaction between cyber operations and international law, in 1990. After a fruitful 20-year career in the US Air Force, Professor Schmitt held the position of Dean of the George C. Marshall European Center for Security Studies and has had a great collaboration with military institutions, namely he is Professor Emeritus at the United States Naval War College and G. Norman Lieberman Distinguished Scholar at West Point. Professor Schmitt was the Director of the Tallinn Manual 2.0, having overseen the original 2013 and is preparing the new volume of this Manual. He is the author of a significant number of important approaches to the interpretation of international law in the realm of cyberspace, and he is a frequently cited expert.

For these reasons, the Military University Institute decided to invite Professor Michael Schmitt to be the keynote speaker at the conference "Military Operations in Cyberspace - New Challenges", which was held on January 06, 2023, with the goal of introducing the Manual of Tallin project and what is expected for the future of this project.

The observations and thoughts shared, always in their incredibly elegant, eloquent, and fluid style, addressed some major issues like the uncertainty over *Jus ad Bellum*, namely the threshold for "use of force" and "armed attack". The debates over the International Humanitarian Law (IHL) regarding the definition of a cyber "attack" and if the data is an "object" and some reflections on the meaning of peacetime/grey area law were also delivered.

For the new volume, as some considerations arose, it was noted the concept of Sovereignty in cyberspace, taking into consideration the interference with, or usurpation of, inherently governmental functions, the due diligence notion as every State has a responsibility to ensure that its territory is not willingly exploited for activities that violate the rights of other States and the collective countermeasures option, as some states accept countermeasures as a lawful response to breaches of international law.

The ambiguity of the States' interpretation of the concepts is a great challenge in the international arena, and the examples presented by Professor Schmitt in this conference were clear to illustrate how different, and sometimes antagonistic, they are.

Following the program in this conference, we had the opportunity to attend a great presentation by Professor José Azeredo Lopes, a former Ministry of National Defence, with the title "Cyber Time and Times of War" where some

themes were readdressed, with few different views. He provided a set of brilliant reflections by the author, namely questioning if cyber is a specific context, the role of third States' offensive cyber operations during a conflict and the role of different kind of Countermeasure, if taken on an individual or collective basis.

After discussing the topic with his deep and assertive posture, Professor Lopes concluded his thoughts making important and significant considerations. On his perspective, we should focus more on State practice accepted as law and its concrete actions on cyber, as much on mere declarations on opinio juris. He also highlighted that in certain cases (v. g., *jus ad bellum*) there can be no strict correspondence between kinetic and cyber "force" and reinforced that there are significant (and natural) differences between levels of public information.

I also highlight the novelty of the presentation by Captain Helder Fialho de Jesus on the Russia-Ukraine conflict, addressing the "international support to Ukraine in cyberspace". He provided his reflexion on this theme where an "International Coalition" to sustain Ukraine in Cyberspace, "led" by the United States, with the collaboration of three Big Tech companies and Starlink, NATO and EU, amongst others, made the difference in this warfare, concluding with the "Civilianization" and "Privatization" of the war. He had also the responsibility for organizing this international conference, supporting the internationalization of this Institute in the military environment.

Therefore, I'd like to note the privilege that it was for everyone to listen to different approaches and reflexions on cyberspace, enriching our knowledge in such important matters.

To all readers, military and civilians, academics, researchers, always curious about this theme, I offer my best wishes for a challenging and fruitful reading.

António Martins Pereira
Lieutenant-General

INTRODUCTION

João Paulo Ferreira Lourenço
Lieutenant-Colonel
Instituto Universitário Militar (IUM) Teacher (1449-027 Lisbon)
lourenco.jpf@ium.pt

In the contemporary theater of conflict, where the digital realm intertwines with geopolitical landscapes, military operations in cyberspace have emerged as a defining frontier. This multifaceted battleground, characterized by the clash of strategic interests, technological prowess, and ideological motivations, is marked by three distinct yet interlinked dimensions: the institutional support extended to Ukraine by countries, organizations, and companies; the phenomenon of hacktivism epitomized by the emergence of IT armies; and the intricate challenge of finding international law in the nebulous domain of cyberspace.

The ongoing conflict between Ukraine and Russia has spurred an unprecedented response in the form of institutional support from a myriad of actors. Nations across the globe, multinational organizations, and tech companies have rallied together, forming a collaborative front to bolster Ukraine's defences in cyberspace. The support ranges from technical expertise and cybersecurity aid to policy collaborations and financial backing, underlining the interconnectedness of the global community in addressing the challenges posed by cyber threats in contemporary conflicts.

Countries such as the United States, European nations, and allies beyond the immediate geographic vicinity of the conflict have played pivotal roles in extending institutional support to Ukraine. The geopolitical implications of this support ripple through the digital landscape, showcasing the significance of alliances and collective defence in the face of evolving cyber threats.

Multinational entities, notably NATO and the European Union, have played crucial roles in coordinating responses, offering policy guidance, and pooling resources to address the multifaceted challenges in cyberspace. The collaborative efforts of these organizations emphasize the necessity of a unified approach in navigating the complexities of modern conflict.

Tech giants and cybersecurity firms have become the vanguards of digital resilience, providing not only technological solutions but also actively engaging in the defense of cyberspace. Their contributions, ranging from threat intelligence to secure communication channels, showcase the vital role that private entities play in fortifying nations against cyber threats.

Amidst the institutional support landscape, a dynamic force emerges – hacktivism, embodied by the rise of IT armies. These groups, comprised of skilled hackers and cyber activists, operate beyond conventional state-sponsored activities, leveraging their technological prowess to advance ideological or political causes. The actions of hacktivist groups transcend the digital realm, influencing narratives, challenging authority, and occasionally aligning with geopolitical conflicts.

The emergence of IT armies marks a paradigm shift in the dynamics of activism. These groups, operating on the fringes of conventional warfare, use their technical acumen to disrupt, expose, and influence. The motivations behind their actions may range from political dissent and advocacy for human rights to challenging oppressive regimes and supporting causes that align with their ethos.

Hacktivism, with its roots in digital activism, has evolved into a formidable force that shapes narratives and impacts geopolitical dynamics. The intersection of hacktivism with institutional support adds an unconventional layer to the digital battlefield, where the motivations of non-state actors intertwine with the strategies of nations and organizations.

As military operations unfold in the intricate landscape of cyberspace, the quest for international law remains an overarching challenge. The absence of clear legal frameworks tailored for the digital realm complicates the attribution of cyberattacks, the definition of thresholds for the use of force, and the establishment of norms governing state behaviour. The challenge of finding international law in cyberspace becomes a paramount concern as conflicts evolve within this intangible and complex domain.

The Ukraine-Russia conflict exemplifies the legal complexities that arise in cyberspace warfare. Traditional legal norms struggle to adapt to the fast-paced evolution of cyber capabilities, raising questions about sovereignty, jurisdiction, and accountability. As military operations extend beyond physical borders, the legal challenges become even more pronounced, demanding a reevaluation of established international legal frameworks.

The quest for international law in cyberspace is not solely a legal challenge but also an ethical imperative. Striking a balance between the imperative to secure nations in the face of cyber threats and safeguarding individual liberties and privacy poses intricate ethical considerations. This exploration delves into the moral complexities inherent in the formulation and application of legal norms in the digital domain.

This book embarks on a holistic exploration of these interconnected realities within the realm of military operations in cyberspace. By dissecting the strategies, motivations, and implications inherent in institutional support, hacktivism, and the quest for international law, it seeks to provide a comprehensive understanding of the evolving nature of conflicts in the digital age.

Through meticulous analysis, case studies, and expert insights, this exploration aims not only to illuminate the nuances but also to foster critical discourse. It serves as a guide for policymakers, legal experts, and practitioners navigating the intricacies of the digital battlefield – where alliances, disruptions, and legal norms converge in shaping the future of conflict in cyberspace.

In the chapters that follow, we will delve deeper into each dimension, unraveling the layers of complexity within institutional support, hacktivism, and the quest for international law in cyberspace. Together, let us navigate the digital landscape and glean insights into the rapidly evolving dynamics of military operations in this complex and dynamic domain.

FINDING INTERNATIONAL LAW IN CYBERSPACE

Professor Michael N. Schmitt
Professor of International Law
University of Reading, West Point, Naval War College, University of Texas, United States
schmitt@aya.yale.edu

Lieutenant-Colonel Durward E. Johnson
Deputy Staff Judge Advocate
V Corps OSJA, Fort Knox, Kentucky, United States
durward.johnson@utexas.edu

1. CYBER OPERATIONS COME OF AGE

The development of international law in cyberspace began in the 1990s. Initially, the focus was on military operations. For instance, the Office of General Counsel at the U.S. Department of Defense prepared the first government assessment of the application of international law to so-called computer network attacks in 1999[1]. Similarly, the first major conference on the topic was held at the United States Naval War College and dealt heavily with questions regarding the use of force (*jus ad bellum*) and international humanitarian law. The conference resulted in an influential edited book on the subject that served as the initial primary reference for those dealing with "computer network attack and exploitation," today commonly labeled cyber operations[2].

Internationally, the first serious consideration of the subject also came in the late 1990s. In 1998, the General Assembly passed Resolution 53/70, a Russian initiative that invited States to share their views on information security and the "advisability of developing international principles that would enhance the security of global information telecommunications systems and help combat information terrorism and criminality."[3] The following year, a Secretary General report included

---

[1] U.S. Department of Defense, Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, (2d ed, Nov 1999), 483-91, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?httpsredir= 1&article=1381&context=ils.

[2] See Michael Schmitt and Brian O'Donnell (eds), "Computer Network Attack and International Law," (2002) 76 *International Law Studies*.

[3] United Nations General Assembly, Fifty-Third Session, *Developments in the field of information and telecommunications in the context of international security*, A/RES/53/70, December 4, 1998, https://documents-dds-ny.un.org/doc/UNDOC/ GEN/N99/760/03/PDF/N9976003.pdf?OpenElement.

the replies of governments[4].

Russia argued that "contemporary international law has virtually no means of regulating the development and application of such a weapon."[5] Therefore, it called for developing principles to govern cyberspace that would "subsequently be incorporated into a multilateral international legal instrument."[6]

The events of September 11th, 2001, and the ensuing armed conflicts in Afghanistan and Iraq, distracted the international legal community's attention, and little progress was made in identifying whether and how international law rules applied in cyberspace. However, in 2007, Estonia was subjected to widespread hostile operations that dramatically disrupted that nation.[7] Although no State could be identified as responsible for the attacks, most cyber operations originated from Russian territory[8]. The fact that Estonia had become a member of NATO in 2004 raised questions about the applicability of Article 5 of the North Atlantic Treaty, the provision providing for collective defense among the Allies.[9] The international legal community had no good answers, for it had been, as noted, preoccupied with the ongoing armed conflicts and counter-terrorism operations. The following year, cyber operations were frequent during the international armed conflict between Georgia and Russia[10]. These operations begged the question of how international humanitarian law governed cyber operations conducted by parties to armed conflict. Again, the international law community had made little progress in understanding this issue during the preceding years.

---

[4] United Nations General Assembly, Fifty-Fourth Session, *Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General*, A/54/213, August 10, 1999, https://documents-dds-ny.un.org/ doc/UNDOC/GEN/N99/235/97/PDF/N9923597.pdf?OpenElement.

[5] A/54/213 at 8.

[6] A/54/213 at 9.

[7] For a thorough discussion on the cyber operations, see Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* 14-33 (Tallinn: Cooperative Cyber Defence Centre of Excellence 2010).

[8] Charles Clover, "Kremlin-backed Group behind Estonia Cyber Blitz," *Financial Times*, March 11, 2009.

[9] For a general timeline of the evolution of NATO's cyber defense strategy, see The NATO Cooperative Cyber Defence Centre of Excellence, *North Atlantic Treat Organisation*, https://ccdcoe.org/organisations/nato/.

[10] See Tikk et al., *International Cyber Incidents*, 66-90 (describing cyber operations against Georgia during the dispute with Russia over South Ossetia).

2. THE TALLINN PROJECT

In the aftermath of these events, a NATO center of excellence was established in 2008[11]. Situated in Tallinn, Estonia, it launched a project to identify how international law applied in cyberspace the next year. A group of 20 experts (the International Group of Experts, IGE) was formed, and one of us (Schmitt) was appointed director[12]. The participants were accomplished legal practitioners and scholars. Many had extensive experience providing legal advice to governments[13]. In addition to the experts, the International Committee of the Red Cross and NATO sent non-voting observers to the project. The IGE decided to take on the two bodies of law that the Estonia and Georgia events had most directly implicated – the *jus ad bellum* and international humanitarian law (IHL)[14]. A few rules of peacetime law were included to provide context.

The work was completed in 2012, and the resulting Tallinn Manual on the International Law Applicable to Cyber Warfare was published the following year[15]. It contained 95 consensus rules together with accompanying commentary that explained the derivation of each rule and points of agreement and disagreement with respect to their application in the cyber context. Initially, it was misunderstood as NATO doctrine and thus evoked opposition from countries such as Russia and China[16]. Nevertheless, the manual quickly became the most influential work on the topic globally. This was among State legal advisers even though there had been no formal State engagement prior to publication because States were concerned about being affiliated with a project they did not control.

---

[11] North Atlantic Treaty Organization, *NATO opens new centre of excellence on cyber defence*, May 14, 2008, https://www.nato. int/docu/update/2008/05-may/e0514a.html.

[12] See The NATO Cooperative Cyber Defence Centre of Excellence, *The Tallinn Manual*, https:// ccdcoe.org/research/ tallinn-manual/.

[13] Although numerous members of the group were serving in senior posts in their countries, all participated in their personal capacity.

[14] Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 Harvard Journal of International Law 13, 2012, p. 16, https://harvardilj.org/2012/12/ online-articles-online_54_schmitt/.

[15] See Michael N. Schmitt, gen. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

[16] For example, see Elena Chernenko, Russia warns against NATO document legitimizing cyberwars May 29, 2013, https://www.rbth.com/international/2013/05/29/russia_warns_against_nato_document_ legitimizing_cyberwars_26483.html; Ashley Deeks, Tallinn 2.0 and a Chinese View on the Tallinn Process, May 31, 2015, http://www.lawfareblog. com/2015/05/tallinn-2-0-and-a-chinese-view-on-the-tallinn-process/.

Although the Tallinn Manual added great clarity to how the *jus ad bellum* and IHL governed cyber operations, several issues in those bodies of law remained unsettled. With respect to the *jus ad bellum*, two were key. The first was the threshold for a "use of force" that is prohibited by Article 2(4) of the UN Charter and customary international law.

The experts agreed that destructive or injurious operations beyond a de minimis level by one State against another qualified[17]. The question was whether cyber operations not having those consequences might ever amount to the use of force and, thus, violate the prohibition[18].

The second issue was situated in the law of self-defense set forth in Article 51 of the UN Charter and customary international law. States have a right to use force when faced with an "armed attack."[19] The notion of armed attack presented the same quandary as that which had arisen in the context of "use of force," identifying where the threshold lies[20]. Most States and the IGE accept the premise set forth by the International Court of Justice in its Nicaragua judgment that an armed attack is the "most grave form" of a use of force[21]. Thus, while all armed attacks are uses of force, not all uses of force are armed attacks for purposes of Article 51[22]. However, the experts were unable to precisely articulate the point at which a cyber use of force, a problematic issue in itself, rises to the level of an armed attack triggering the right of self-defense[23].

With regard to IHL, two unsettled issues loomed large. Most problematically, consensus could not be reached on when a cyber operation by one party to an armed conflict qualified as an "attack," as that term operates in IHL[24]. The issue is critical because many of the conduct of hostilities prohibitions, limitations, and

---

[17] See *Tallinn Manual*, 47.
[18] The U.N. Charter contains two exceptions to the prohibition to the use of force – uses of force authorized by the Security Council pursuant to Article 42 and self-defense in accordance with Article 51.
[19] U.N. Charter art. 51; *Tallin Manual 2.0*, rule 71.
[20] See *Tallinn Manual*, 55
[21] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States), Judgment, 1986 I.C.J. Rep. 14, para. 191 (June 27)
[22] The U.S. takes the position that any unlawful use of force qualifies as an armed attack, thus on this view there is no gap between an unlawful use of force and an armed attached. See, e.g., Department of Defense, Law of War Manual, para. 16.3.3.1; see also Abraham D. Sofaer, "International Law and the Use of Force," 82 *American Society of International Law Proceedings* 420, 422 (1988).
[23] See *Tallinn Manual*, 55.
[24] See *Tallin Manual*, 92-94. It is critical to differentiate the term "attack" as a term of art in IHL from the term "armed attack" as used as a condition precedent for purposes of self-defense under Article 51 of the U.N. Charter.

requirements attach only to operations that amount to an attack. For instance, if a cyber operation is not an attack under IHL, it may be directed at civilian cyber infrastructure[25].

The term is defined in Additional Protocol I to the 1949 Geneva Conventions as an "act of violence, whether in offense or defense."[26] Thus, the experts concluded that destructive and injurious cyber operations conducted during an armed conflict were attacks subject to such rules as prohibitions on attacking civilians or civilian objects, the rule of proportionality, and the requirement to take precautions in attack[27]. The question they could not answer was whether cyber operations not having these effects were nevertheless subject to IHL's attack rules.

Most of them agreed that a cyber operation that interfered relatively permanently with the functionality of cyber infrastructure qualified[28]. For example, if a cyber operation required the replacement of components of the targeted system, the operation is an attack. The experts cited an example of a cyber operation against an electrical distribution grid's computer-based control system in which functionality can only be restored by replacement of the system or its components. No consensus, or even a majority perspective, could be identified for cyber operations having consequences below this level, such as data restoration or reinstallation of an operating system.

The second issue the experts struggled with was whether data qualifies as an "object" in the IHL context[29]. It is a question that is central to cyber targeting during an armed conflict because IHL prohibits attacks against civilian objects and requires harm to those objects be considered when making proportionality determinations and assessing the feasibility of precautions in attack[30]. Two competing views emerged. By the first, data is not an object because it is not

---

[25] The principle of distinction is a customary law principle requiring parties to an armed conflict where IHL applies shall distinguish between civilian objects and military objectives, and only direct operations against military objectives. See Jean-Marie Henckaerts & Louise Doswald Beck, 1 Customary International Law Study 59-158 (International Committee of the Red Cross, 2005). This principle is also reflected in article 48 of the Additional Protocol I. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 48 June 8, 1977, 1125 U.N.T.S. 3.

[26] Additional Protocol I, art. 49(1).

[27] See *Tallinn Manual*, 92.

[28] See *Tallinn Manual*, 93-94.

[29] See T*allinn Manual*, 187.

[30] Additional Protocol I, arts. 52, 57; see also Eric Talbot Jensen, "Cyber Attacks: Proportionality and Precautions in Attack," 89 *International Law Studies* 198 (2013).

"tangible." The problem with this approach is that it left too much on the table. It would, for instance, permit cyber operations against any civilian database so long as they did not, in turn, generate physical damage or injury. The alternative view is that data should be treated as an object. But this approach took too much off the table, for militaries have long conducted psychological operations designed to influence the civilian population. In the 21st century, such operations may take the form of cyber operations that affect data. This debate continues to rage, a reality that has led one of us to recommend a policy remedy until consensus can be achieved[31].

Of course, the most significant question remaining following the publication of the first Tallinn Manual was how international law governed cyber operations not occurring during an international or non-international armed conflict. This led to the second phase of the project, in which a new IGE tackled that issue. Beginning in 2013, the 20 experts, assisted by a NATO observer who did not have the right to vote but was free to comment upon the discussions, considered issues ranging from sovereignty in cyberspace to the applicability of space law to cyber operations mounted into, from, or through outer space. They combined their work with a slight rewrite of the first Tallinn Manual to produce 154 rules with accompanying commentary[32].

Importantly, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations was published only after extensive formal State engagement. The Netherlands Ministry of Foreign Affairs hosted three sessions in The Hague at which States, and international organizations discussed draft text with the project's leadership and offered many suggestions for revision[33]. Additionally, all States were afforded the opportunity to provide written comments on that text. Many States did so in great depth. The IGE took those comments into consideration before publication of the final draft in 2017.

The international response to Tallinn Manual 2.0 was very positive. Many States appear to have relied heavily upon it in issuing their statements on the state

---

[31] See Michael N. Schmitt, "Wired warfare 3.0: Protecting the civilian population during cyber operations," *International Review of the Red Cross* (2019), 333-355, https://international-review.icrc.org/articles/wired-warfare-30-protecting-civilian-population-during-cyber-operations.
[32] See Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).
[33] See *Tallinn Manual* 2.0, 6.

of international law in cyberspace[34]. Some have done so by expressly referring to aspects of the manual[35]. Indeed, in its June 2018 resolution on cyber defense, the European Parliament noted "the relevance of the Tallinn Manual 2.0 as a basis for a debate and as an analysis of how existing international law can be applied in cyberspace; [and] call[ed] on the Member States to start analysing and applying what the experts have stated in the Tallinn Manual."[36] Today, it is fair to say that it is the most influential work on the subject for both practitioners and scholars.

The IGEs that prepared both manuals were committed to the premise that States make and authoritatively interpret international law, not academics. Therefore, as States began to generate positions on the points the experts had addressed, the currency of the conclusions and interpretations found in Tallinn Manual 2.0 diminished. As a result, the decision was taken to launch a third Tallinn Manual iteration[37].

The Tallinn Manual 3.0 process will have three tasks in light of the growing body of State actual and "verbal" practice, such as NATO doctrine, the statements

---

[34] See, e.g., Republic of Finland, Ministry of Foreign Affairs, *International Law and Cyberspace: Finland's National Positions*, October 15, 2020, https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t= 1603097522727; Federal Republic of Germany, Ministry of Defense, *On the Application of International Law to Cyberspace*, March 2021, https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/ on-the-application-of-international-law-in-cyberspace-data.pdf; Government of Netherlands, [Letter from the] Minister of Foreign Affairs to the President of the House of Representatives, *Appendix*: *International law in cyberspace*, July 5, 2019, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/ 09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace; Government of Australia, 2020 International Cyber and Critical Technology Engagement Strategy, *Annex B: Australia's position on how international law applies to State conduct in cyberspace* (2020), https://www.international cybertech.gov.au/our-work/annexes/annex-b; Government of New Zealand, Ministry of Foreign Affairs and Trade, *The Application of International Law to State Activity in Cyberspace* (2020), https://www.mfat.govt.nz/en/media-and-resources/ the-application-of-international-law-to-state-activity-in-cyberspace/; Republic of France, Ministry of the Armies, *International Law Applied to Operations in Cyberspace* (2019), https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf;

[35] See, e.g., the contributions of Germany, Japan, and the Netherlands in the United Nations General Assembly, Seventy-Six Session, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution* 73/266, A/76/136, July 13, 2021, https://documents-dds-ny.un.org/doc/ UNDOC/GEN/N21/ 189/48/PDF/N2118948.pdf?OpenElement. [hereinafter *2021 GGE Compendium*]

[36] European Parliament, *European Parliament resolution of 13 June 2018 on cyber defence*, Resolution 2018/2004(INI), June, 13, 2018, para. 47, https://www.europarl.europa.eu/doceo/document/TA-8-2018-0258_EN.html.

[37] See The NATO Cooperative Cyber Defence Centre of Excellence, *The Tallinn Manual*, https://ccdcoe.org/research/ tallinn-manual/.

of individual States, and the work of the international community, especially in the UN's Group of Governmental Experts and Open-Ended Working Group on international communications technology (ICT)[38]. First, based on this State practice, a new team will reexamine contentious issues from the first and second manuals. Second, it will use the State practice to refine and develop the existing analysis of even uncontroversial positions. Finally, the drafters will identify areas of international law that were not treated at all or with sufficient depth and develop text on them. For instance, international criminal law will have much greater prominence in the new work.

3. THE WORK AHEAD

As the project is ongoing, it is impossible to definitively describe the changes that will be made. However, various issues of international law will loom large. The most prominent include the following.

Sovereignty. Both the first and second IGEs concluded that a rule of sovereignty governs activities in cyberspace[39]. That rule is violated in two circumstances. First, a remotely conducted cyber operation by or attributable to one State into the territory of another violates the rule of territorial sovereignty when certain effects occur. Consensus was not achievable on the qualifying effects. Still, there was agreement that sovereignty operated in this manner and that at least cyber operations that caused injury, physical damage, or relatively permanent loss of functionality of the affected cyber infrastructure qualified as a violation[40].

The second means of violating the target State's sovereignty is by interfering with or usurping that State's inherently governmental functions. Inherently governmental functions are activities that only States have the right under international law to engage in or delegate to non-State actors. In the cyber context, the paradigmatic example is the conduct of elections[41]. Other examples include the

---

[38] See United Nations General Assembly, Seventy-Third Session, *Advancing responsible State behaviour in cyberspace in the context of international security*, A/RES/73/266, December 22, 2018, https://documents-dds-ny.un.org/doc/UNDOC/ GEN/N18/465/01/PDF/N1846501.pdf?OpenElement; and *Developments in the field of information and telecommunications in the context of international security*, A/RES/73/27, December 5, 2018, https://documents-dds-ny.un.org/doc/UNDOC/ GEN/N18/418/04/PDF/N1841804.pdf?OpenElement.

[39] See *Tallin Manual*, 25-35; and *Tallin Manual 2.0*, rule 1.

[40] See *Tallin Manual 2.0*, rule 4, paras. 11-13.

[41] For an in-depth discussion on cyber interference in elections, see Michael N. Schmitt, "Foreign Cyber Interference in Elections," 97 *International Law Studies* 740-764 (2021).

collection of taxes and national defense. Again, although a degree of uncertainty remains as to the precise parameters of the notion of an inherently governmental function and the extent of interference that triggers the prohibition, there was general consensus that the rule operated in this manner[42].

Surprisingly, in 2018 the U.K. Attorney General, in a speech at Chatham House, stated, "I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The U.K. Government's position is therefore that there is no such rule as a matter of current international law."[43] The United Kingdom's rejection of sovereignty as a rule of international law applicable to cyber operations was reaffirmed most recently in 2022[44].

In this regard, the United Kingdom is figuratively an island. It is the only State that has unambiguously adopted the position. While many States have either affirmed the principle, as distinct from the rule, of sovereignty or remain silent, every State that has spoken directly to the issue has rejected the British position[45]. Even some so-called "Five Eyes" States have done so. For instance, Canada has stated that "it is axiomatic that the principle of sovereignty applies in cyberspace, just as it does elsewhere."[46] And Allied Joint Publication 3.20, Cyber Operations, provides, "Depending on the context, such COs may nevertheless constitute a violation of international law as a breach of sovereignty or other internationally wrongful act."[47] The United Kingdom reserved on the statement, but no other country, including the United States, did so[48].

---

[42] See *Tallin Manual 2.0*, rule 4, paras. 15-18.
[43] Jeremy Wright, Attorney General, United Kingdom, *Cyber and International Law in the 21st Century*, Chatham House (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century
[44] Suella Braverman, Attorney General, United Kingdom, *International Law in Future Frontiers*, Chatham House (May 19, 2022), https://www.gov.uk/government/speeches/international-law-in-future-frontiers; see also the contribution of the United Kingdom of Great Britain and Northern Ireland in the 2021 GGE Compendium, para. 10 pg. 117.
[45] See, e.g., Netherlands, *International Law in Cyberspace, at 2; Finland, International Law and Cyberspace*, at 3; New Zealand, International Law to State Activity in Cyberspace, paras. 11-15.
[46] Government of Canada, Global Affairs Canada, *International Law applicable in cyberspace* (2022), para. 10, https:// www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/ cyberspace_law-cyberespace_droit.aspx?lang=eng#a3.
[47] NATO, Ministry of Defence, AJP–3.20 (ed. A, v. 1), *Allied Joint Doctrine for Cyberspace Operations* (2020), fn. 26 to para. 3.7, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/ doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.
[48] See AJP–3.20, pg. v.

Nevertheless, because of the prominent role of the United Kingdom in cyberspace, the issue of sovereignty remains a topic of discussion. It will be addressed fully in Tallinn Manual 3.0. We anticipate that over time the British position on the matter will soften, for, in our estimation, the legal basis for rejecting the rule of sovereignty is tenuous, and the weight of opinion is overwhelmingly on the side of its existence[49].

Due Diligence. The rule of due diligence was perhaps best defined by the International Court of Justice in its first case, Corfu Channel (1949)[50]. There, the Court noted that "[I]t is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[51] Building on that case and its treatment in the ensuing years, the Tallinn Manual 2.0 experts adopted two due diligence rules[52]. According to Rule 6, which expresses the general principle, "a State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its government control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States." Rule 7 requires States to "take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States." For the experts, the rules encompass many hostile cyber operations by States or non-State actors that are either conducted remotely using infrastructure in an intermediary State or conducted by them from that State.

Although the experts were unanimous in their conclusion that such a rule of international law existed[53] and that the challenge would be determining precisely how it does so in the complicated cyber context, those States that have addressed the issue head-on are split. A number of them have adopted the Tallinn Manual 2.0 approach. For instance, the Netherlands has consistently regarded "the principle as an obligation in its own right, the violation of which may constitute an internationally wrongful act."[54] Similarly, Germany has stated that the rule of

---

[49] For thorough discussion on the subject, see Michael N. Schmitt & Liis Vihul, "Sovereignty in Cyberspace: Lex Lata Vel Non?," 111 *American Journal of International Law Unbound* 213, 213–14 (2017); see also Kevin Jon Heller, "In Defense of Pure Sovereignty in Cyberspace," 97 *International Law Studies* 1433-1498 (2021); see also the majority of State contributions in the *2021 GGE Compendium*.
[50] *The Corfu Channel Case* (United Kingdom v. Albania), Judgment, 1949 I.C.J. 4 (April 9).
[51] *Corfu Channel*, pg. 22.
[52] *Tallinn Manual 2.0*, rules 6, 7.
[53] *Tallinn Manual 2.0*, rule 6, paras. 3, 4.
[54] See Netherlands, *International Law in Cyberspace*, at 4; see also the Netherlands contribution in the *2021 GGE Compendium*, pg. 59.

due diligence is "widely recognized in international law, is applicable to the cyber context as well and gains particular relevance here"[55].

But in 2021, Israel argued that "[w]e have not seen widespread State practice beyond this type of voluntary cooperation, and certainly not practice grounded in some overarching opinio juris."[56] All "Five-Eyes" States (U.S., U.K., Canada, Australia, and New Zealand) agree. However, they have not ruled out the possibility that such a rule might emerge in the future or that through continued study of the matter[57]. Their position is that more State practice (actual and verbal) is needed before due diligence crystallizes into a norm of customary international law[58].

In our estimation, that conclusion is questionable. It has long been the case that international law rules and principles apply to new technologies. This was the International Court of Justice's finding in its Nuclear Weapons advisory opinion[59].

Similarly, IHL requires new weapons to be assessed for legality in light of existing international law[60]. Thus, the correct starting point is that the rule of due diligence applies in the cyber context. It is only when a State determines in good faith that the application of the rule to a new technology is either unreasonable (due to unique characteristics of the technology) or would run counter to the object and purpose of the rule that it may credibly assert that the technology is not governed by existing law[61]. States opposing the existence of a due diligence rule have not made either assertion with any specificity.

Moreover, in terms of policy, due diligence is a sensible rule to embrace. For instance, it allows States that are the target of hostile non-State cyber operations emanating from another State to respond with countermeasures if the State

---

[55] See the German contribution in the *2021 GGE Compendium*, section II(a) pg. 33.
[56] Roy Schöndorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations," 97 *International Law Studies* 395, 404 (2021).
[57] See, e.g., Canada, *International Law in Cyberspace*, fn 20 to para. 26.
[58] For example, see the contributions of the United States pg. 141, United Kingdom para. 12 in the *2021 GGE Compendium*.
[59] Advisory Opinion, *Legality of the Threat or Use of Nuclear Weapons*, 1996 ICJ 226 (July 8), para. 86 (the principles and rules of IHL "appl[y] to…all kinds of weapons, those of the past, those of the present and those of the future.).
[60] See Additional Protocol I, art. 36; see also DOD Law of War Manual, para. 6.2.3.
[61] See Vienna Convention on the Law of Treaties, art. 31(1), opened for signature May 23, 1969, 1155 U.N.T.S. 331. While the concepts are found in the law of treaty interpretation, the logic is no less applicable to applying it to customary rules of international law; On the comparison between interpretation of customary and treaty rules, see Marina Fortuna, Different Strings of the Same Harp Interpretation of Customary International Law versus Identification of Custom and Treaty Interpretation, in The Theory, Practice and Interpretation of Customary International Law (Paros Merkouris, Jörg Kammerhoffer & Noora Arajärvi eds., 2022)

from which the cyber operations originate is unwilling to terminate those cyber actions[62]. Countermeasures are actions that would be unlawful but for the fact that they are intended to compel another State back into compliance with international law[63]. Countermeasures are only available against a State that has committed an internationally wrongful act, not against a non-State actor[64]. However, if a non-State actor is operating from or through another State and that State fails to take feasible measures to put an end to those operations, the victim State may employ countermeasures to compel the territorial State to act because it is now in breach of its due diligence obligation. These measures may take the form of operations designed to influence the territorial State to put an end to the hostile operations or to directly shut down the non-State actor's systems[65].

As cyber operations from or through a State that is not responsible for them grow in frequency and severity, a due diligence obligation will inevitably become more appealing. After all, it allows victim States to insist that territorial States take action to put an end to the harmful operations in situations where the victim State itself may not be legally entitled or practically able to do so. Additionally, what is often missed by States that oppose the due diligence rule is that it only applies to ongoing hostile operations; it does not require States to take preventive measures[66]. Moreover, the obligation is satisfied so long as the territorial State takes feasible measures[67]. The rule does not obligate States to take actions that would be unduly difficult in the circumstances. Thus, for instance, the territorial State does not have to acquire the cyber capability to act against hostile operations from its territory, and factors such as expense or impact upon cyber activities in the territorial State may render action unfeasible.

Collective Countermeasures. As noted, countermeasures are otherwise unlawful actions taken in response to a violation of international law (an internationally wrongful act) by another State; qualification as a countermeasure is what is known in international law as a "circumstance precluding wrongfulness."[68]

---

[62] See *Tallinn Manual 2.0*, rule 7 para. 28.
[63] See *Tallinn Manual 2.0*, rule 21.
[64] See *Tallinn Manual 2.0*, rule 20.
[65] See Michael N. Schmitt, "In Defense of Due Diligence in Cyberspace," 125 *Yale Law Journal Forum* 68, 79 (2015), http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in cyberspace.
[66] See *Tallinn Manual 2.0*, rule 7 paras. 7-10.
[67] See *Tallinn Manual 2.0*, rule 7 para. 2.
[68] International Law Commission, Fifty-third session, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, A/56/10, November 2001, art. 49-54.

The Tallinn Manual 2.0 IGE concluded that they were available in the cyber context and devoted much attention to their use[69]. And no State has objected to applying the law surrounding countermeasures in the cyber context. Thus, the IGE relied upon the International Law Commission's restatement of that law in its Articles on State Responsibility in drafting its cyber-relevant countermeasures rules.

Of course, various aspects of the countermeasures discussion will need slight revision in Tallinn Manual 3.0. However, one contentious issue has arisen and is of great significance for NATO – collective countermeasures. In the law of self-defense, States are entitled to use force in the collective defense of a State that is the victim of an armed attack, so long as the victim State asks it to do so[70]. The question concerning countermeasures is whether States may similarly come to the aid of a State targeted by a third State's internationally wrongful cyber operations when the assistance would otherwise be unlawful. For instance, may a State that is the victim of unlawful cyber operations by another State turn to a friendly State that is more cyber capable and ask it to hack back against its attacker even though the hack back would violate the sovereignty of the malevolent attacking State?

Very few States have spoken to this issue. The controversy arose when the Estonian President made a speech at the 2019 CyCon conference asserting that "[S]tates which are not directly injured may apply countermeasures to support the State directly affected by the malicious cyber operation."[71] However, the same year, the Ministry of the Armies of NATO ally France took the opposite position. It asserted that "Collective countermeasures are […] not authorized, which excludes the possibility for France to adopt such measures in response to a violation of the rights of a third State."[72] This is a significant disagreement because NATO allies may wish to cooperate in the face of hostile cyber operations that have not yet reached the armed attack level that triggers collective self-defense under Article 5 of the North Atlantic Treaty[73].

In our view, both positions are reasonable, but the more defensible one is that which Estonia originally offered. To the extent States may use force in support

---

[69] See *Tallinn Manual 2.0*, rules 20-25.
[70] U.N. Charter art. 51.
[71] Kersti Kaljulaid, President of Estonia, Opening at CyCon 2019 (May 29, 2019), https://news.err.ee/946827/ president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon.
[72] France, *International Law in Cyberspace*, para. 1.1.3.
[73] North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243; see generally Michael N. Schmitt, "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law," 54 *Virginia Journal of International Law* 697 (2013).

of each other, they should be entitled to employ measures short of the use of force. Indeed, effective countermeasures may preclude the escalation of a situation to the armed attack level. We would also note that States lacking robust cyber capability would be well advised to support the premise that collective countermeasures are permissible for the position precludes them from being defenseless in the face of hostile cyber operations by other States[74].

As to why some States might object to the notion of collective countermeasures, the most likely practical reason is that their availability could pose a dilemma should they be asked to support another State with countermeasures. On the one hand, the State might fear becoming embroiled in the situation. On the other, it may not want to appear to have denied assistance to a friendly State in its time of need. It is much easier to simply adopt the position that qualification of a cyber operation as a countermeasure precludes only the wrongfulness of action taken by the State targeted by hostile cyber operations, not other States.

Use of Force. As discussed above, the central unresolved issue regarding the prohibition on the use of force that remained following the publication of the first Tallinn Manual (and second) was the threshold at which a cyber operation qualifies as a use of force and is, therefore, unlawful unless conducted in response to an armed attack according to the law of self-defense, or authorized or mandated by the Security Council under Chapter VII of the UN Charter. In Nicaragua, the International Court of Justice articulated an approach with respect to determinations that non-kinetic operations could qualify, in certain circumstances, as a use of force, thus leading to the conclusion that non-destructive cyber operations could sometimes amount to a use of force[75]. Yet, uncertainty regarding the precise threshold abounds.

Both Tallinn Manual IGEs adopted a "scale and effects" approach initially suggested in a 1999 article by one of the authors[76], according to which States are likely to refer to a variety of non-exclusive factors in making the assessment[77]. As outlined in Tallinn Manual 2.0, those factors include severity, immediacy, directness, invasiveness, measurability of effects, military character, state

---

[74] For an in-depth discussion on the issue, see Michael N. Schmitt and Sean Watts, "Collective Cyber Countermeasures?," 12 *Harvard National Security Journal* 176 (2021).
[75] *Nicaragua*, para. 228.
[76] See Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law," 37 *Columbia Journal of Transnational Law* 885 (1999).
[77] See *Tallinn Manual*, 47-52; see also *Tallinn Manual 2.0*, rule 69 para. 8-10.

involvement, and presumptive legality[78]. Depending on the circumstances, other factors States may consider involve the prevailing political environment, whether the cyber operation presage the future use of military force, the identity of the attacker, any record of cyber operations by the attacker, the nature of the target (like critical infrastructure), and the number of factors acting in concert at any given time[79].

States are speaking to this issue. There appears to be an emerging consensus that the appropriate approach is to consider the "scale and effects" of the hostile cyber operation in determining whether it reached the use of force threshold[80]. The discussion of the subject in NATO's 2020 doctrine for cyber operations is illustrative. It observes, "Criteria that could be considered in making this assessment include the scale and effects of the attack, which might take into account such factors as interference with critical infrastructure or functionality, severity and reversibility of effects, the immediacy of consequences, the directness between act and consequences, and the invasiveness of effects."[81] Some of these factors are taken verbatim from Tallinn Manual 2.0. At the time, 30 nations were members of the Alliance, and none objected to this text in Allied Joint Publication 3.20[82].

Tallinn Manual 3.0 will necessarily have to take account of these statements. Although it is premature to offer a definitive conclusion on the matter, we anticipate that support for the scale and effects approach and its reliance on a variety of non-exclusive factors will continue to grow.

Armed Attack. There is no reason to believe the same approach will not be adopted for evaluating a cyber operation against the armed attack threshold that allows for using force in individual or collective self-defense. Indeed, the fact that States are adopting the "scale and effects" test to assess the use of force signals their acceptance of it when determining whether the right of self-defense has been triggered. Although fewer States have expressed an opinion on how to make that assessment, there is no reason to believe that factors like those States have begun

---

[78] See *Tallinn Manual 2.0*, rule 69 para. 9.
[79] See *Tallinn Manual 2.0*, rule 69 para. 10.
[80] For examples, see the State contributions in the *2021 GGE Compendium*; see also, e.g., Canada, *International Law in cyberspace*, para. 45; New Zealand, *International Law to State Activity in Cyberspace*, paras. 7; and Finland, *International Law and Cyberspace*, at 6.
[81] See AJP–3.20, para. 3.7.
[82] Only the United Kingdom and the United States recorded reservations and none regarding this specific issue, see AJP–3.20, pg. v.

to cite for use of force "scale and effects" determinations will not apply mutatis mutandis to armed attack determinations. Of course, since an armed attack is the "most grave" form of the use of force, those factors will be more demanding[83].

States may argue that they are so demanding that only physical destruction or death suffices. But the one State that has spoken directly to the issue, France, raised the prospect of cyber operations not having such consequences nevertheless qualifying as an armed attack. Of note is its willingness to treat certain operations generating economic harm as doing so: "A cyberattack could be categorized as an armed attack if it caused substantial loss of life or considerable physical or economic damage. That would be the case of an operation in cyberspace that caused a failure of critical infrastructure with significant consequences or consequences liable to paralyze whole swathes of the country's activity, trigger technological or ecological disasters and claim numerous victims."[84]

It seems logical that other States would treat a devastating economic cyberattack as allowing for the resort to force in self-defense. However, except for France, none have expressly adopted that position, although both Singapore and Norway have gone as far as accepting the possibility that economic harm may qualify as an armed attack[85]. The Tallinn Manual 3.0 drafting team is carefully monitoring verbal State practice on this issue.

International humanitarian law. Since the publication of Tallinn Manual 2.0, there has been little resolution of the two contentious issues discussed above. States recognize the challenges they present and have taken sides, but no side appears to be prevailing. To illustrate, it is helpful to compare France's positions with Israel's.

Concerning the qualification as an attack (such that one against a civilian object would be unlawful), France is of the view that a cyber operation causing the targeted system to "no longer provide the service for which they were implemented, whether temporarily or permanently, reversibly or not" is an attack[86]. In other

---

[83] See *Nicaragua*, para. 191, where the ICJ expressed that armed attacks were merely "the most grave forms of the use of force."
[84] France, *International Law in Cyberspace*, para. 1.2.1.
[85] See the Singapore contribution in the 2021 GGE Compendium, pg. 84 para. 8, noting "a targeted cyber operation causing sustained and long-term outage of Singapore's critical infrastructure" may be considered an armed attack; and the Norway contribution in the 2021 GGE Compendium, pg. 77 para. 3.3, noting "[a] cyber operation that severely damages or disables a State's critical infrastructure or functions may furthermore be considered as amounting to an armed attack under international law."
[86] See France, *International Law in Cyberspace*, para. 2.2.1.

words, France has adopted the loss of functionality approach. By contrast, Israel takes the position that "mere loss or impairment of functionality to infrastructure would be insufficient" to qualify a cyber operation as an attack under IHL[87]. By its interpretation, cyber operations targeting civilian systems would have to generate physical damage or injury to amount to an attack subject to IHL's rules on attacks.

Similarly, France takes a broad view by which content data is an object, whereas Israel rejects that position[88]. As noted, we believe both positions are unsatisfactory in certain circumstances. The former is flawed because it will preclude certain operations by cyber means that have long been conducted in the non-cyber context, especially psychological operations. The latter view is troubling because it would allow a party to a conflict to create exceptional hardship for its opponent's civilian population without physically harming it[89]. It is important to note in this regard that Israel observes that if an operation against data has a destructive knock-on effect on civilian objects, the operation would be unlawful as an attack on a civilian object[90].

4. CONCLUSION

The application of international law to cyber will evolve as States continue to generate positions on its application. At the forefront of helping to influence the developing body of law and State interpretations will be the new Tallinn Manual, the original 2009 version of which sparked the development of international law in cyberspace. Due to a growing body of State practice (both actual and "verbal," i.e., statements and official positions of States), the currency of the conclusions and interpretations set forth in the second iteration of the Tallinn Manual has diminished since 2017, thus necessitating further refinement and exploration of how international law governs cyberspace.

The exact contours of the substantive changes that will be adopted in Tallinn Manual 3.0 cannot be predicted. What is known is that the project will involve a new team to reexamine the contentious issues left unresolved in the first and second

---

[87] See Schöndorf, "Israel's Perspective," 400.
[88] Compare France, *International Law in Cyberspace*, para. 2.2.2; and Schöndorf, "Israel's Perspective," 401.
[89] See *Tallinn Manual 2.0*, rule 100 paras. 6, 7.
[90] Schöndorf, "Israel's Perspective," 401, noting that cyber operations "involving the deletion or alteration of computer data is still reasonably expected to cause physical damage to objects or persons" may be considered an attack subject to IHL targeting rules.

manuals, incorporate State practice to refine and develop the existing analysis n the manuals, and identify areas of international law that need further development or were not dealt with, such as international criminal law. Ultimately, the goal of the project is to play an influential role in the continuing State and academic dialogue regarding how international law applies to cyber operations. If the Tallinn Manual 3.0 project can continue to help States reach common understandings, the international community will be one step closer to ensuring security across the entire cyber domain.

AUTHOR's POSTFACE

Professor Schmitt is Professor of International Law at the University of Reading in the United Kingdom. He is also the G. Norman Lieber Distinguished Scholar at West Point and Charles Stockton Distinguished Scholar-in-Residence and Professor Emeritus at the United States Naval War College. The General Editor of the Lieber Studies (Oxford UP), he previously served as Professor of International Law at Durham University and the University of Exeter, Dean of the George C. Marshall European Center for Security Studies in Germany, and General Editor of International Law Studies and the Yearbook of International Humanitarian Law. Before joining the Marshall Center, Professor Schmitt served 20 years in the United States Air Force as a judge advocate specializing in operational and international law.

Lieutenant Colonel Durward E. Johnson is the Deputy Staff Judge Advocate, V Corps. He previously served as the Chief of Military Justice, III Corps and Fort Hood, Texas. He was also the Associate Director for Law of Land Warfare and Professor of International Law at the Stockton Center for International Law and the U.S. Naval War College in Newport, Rhode Island as well as the U.S. Army's senior operational law trainer at the Joint Multinational Readiness Center, Hohenfels, Germany. He has also been a legal advisor deployed in support of military operations in Afghanistan and Iraq. LTC Johnson holds an LL.M. in Military Law from The Judge Advocate General's Legal Center & School, a J.D. from Loyola Law School, Los Angeles, and a Bachelor of Science from the University of Texas at Austin.

CYBER TIME AND THE TIMES OF WAR

José Alberto Azeredo Lopes
Professor of International Law
Católica Porto School of Law, Portugal
Blanquerna, Barcelona, Spain
jlopes@ucp.pt

1. INTRODUCTION - DIFFERENT WORLDS IN PERSPECTIVE

Is the cyber domain a domain of operations, and how does international law apply to it? The question may seem an exercise of rhetoric (and probably it is), considering what was solidly accepted years ago by NATO[91], what States have since then declared in Law of Armed Conflict (LOAC) Manuals[92], and the opinion of most international lawyers. As NATO's Secretary-General said in 2016, we agreed that we will recognise cyberspace as an operational domain. Just like air, sea and land. Cyber defence is part of collective defence. Most crises and conflicts today have a cyber dimension. So treating cyber as an operational domain would enable

[91] At the Wales Summit, in 2014, Allies began affirming 'that cyber defence is part of NATO's core task of collective defence', *Wales Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, par. 72 https://www.nato.int/cps/en/natohq/official_texts_112964.htm. Two years later, another move was achieved at the Warsaw Summit when NATO Members recognized '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' and agreed to implement a Cyber Defence Pledge, *Warsaw Summit Communiqué, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*, pars. 70–71 https://www.nato.int/cps/en/natohq/official_texts_133169.htm. From that moment onward, more declarations were made. Just to name some examples, in Brussels in 2018, an increasing number of cyber threats were acknowledged by the Head of States and full commitment on the implementation of the Cyber Defence Pledge was reaffirmed, *Brussels Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018*, par. 20 https://www.nato.int/cps/en/natohq/official_texts_156624.htm. And in 2021, NATO Summit in Brussels, Heads of State and Government endorsed NATO's Comprehensive Cyber Defence Policy, *Brussels Summit Communiqué, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021*, par. 32 https://www.nato.int/cps/en/natohq/news_185000.htm. At an operational level, it is worth noting the NATO Cyber Security Centre (NCSC), based at Supreme Headquarters Allied Command Europe (SHAPE) in Mons, Belgium. Also, in terms of international cooperation, cyber defence is one of the areas of strengthened cooperation between NATO and the EU.

[92] See, more recently, Ministerio de Defensa, 'Derecho Internacional Humanitario (DIH) en las FAS' (2022) Madrid, chapter IV (*Conducción de hostilidades*), 103–127 https://publicaciones.defensa.gob.es/media/downloadable/files/links/p/d/pdc_02.01_derecho_internacional_humanitario_fas.pdf

us to better protect our missions and operations[93].

Nevertheless, there are some challenges in applying the consequences normally attached to kinetic threats, to the use of force (or to its most serious violations, such as an armed attack), to cyber operations[94] or cyberattacks. The criterion of 'scale and effects' is the cornerstone of most evaluations[95], and the Portuguese National Cyberdefence Strategy, adopted in November 2022, follows this pattern[96]. Nevertheless, my point is that the idea of '*as if it was*' has its limits.

Regardless of the apparent theoretical consensus, it is difficult, if not impossible, to give clear examples of autonomous cyber operations that should have been qualified as a threat or use of force under article 2, 4 of the United Nations Charter[97], or even less to allow a response to it as self-defence under article 51 of

---

[93] Press conference, NATO Secretary General Jens Stoltenberg following the North Atlantic Council meeting at the level of NATO Defence Ministers, 14 June 2016, https://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en.

[94] PAUL DUCHEINE AND PETER PIJPERS, 'The Notion of Cyber Operations' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (2nd edn, Elgar 2023, 272–296).

[95] See TALLINN MANUAL, Rule 71, *Self-defence against armed attack*, 'A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects'. See also ICJ, *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States of America), Judgement, Merits, 27 June 1986, 103, par. 195 (in which the 'scale and effects' is established considering a substantially different situation): '[t]he Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces.'

[96] Resolução do Conselho de Ministros 106/2022, 'Aprova a Estratégia Nacional de Ciberdefesa', DR 211/2022, Série I, 2/11/2022, 13–22 https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/106-2022-202899924.

[97] On the customary nature of article 2, 4 and its recognition by the ICJ (*in Nicaragua and the Wall* Advisory Opinion), see MARCO ROSCINI, 'Cyber Operations as a Use of Force', *Research Handbook on International Law and Cyberspace*, 2nd edition, Edward Elgar Publ., 2021, 297-316. The ILC considers that the prohibition of aggression is a peremptory norm of general international law. See Draft conclusions on identification and legal consequences of peremptory norms of general international law (jus cogens), 2022, conclusion 23, Annex, a) https://legal.un.org/ilc/texts/instruments/english/draft_articles/1_14_2022.pdf. See also DAN EFRONY AND YUVAL SHANY, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 AJIL 583–657, and *contra*, NICHOLAS TSAGOURIAS, 'The Slow Process of Normativizing Cyberspace' (2019) 113 AJIL 71–75.

the Charter. This can be confirmed with a very thorough analysis of real examples[98], even if some are considered to be scenarios of 'automatic' cyber defence[99].

On the one hand, Germany, for instance, declares that 'cyber operations might fall *in extremis* within the scope of the prohibition of the use of force and thus constitute a breach of article 2 par. 4 UN Charter'[100]. Brazil, on the other hand, has recently stated that '[i]t is generally understood that, to date, no State has claimed that the rule prohibiting the use of force was violated due to the conduction of a cyberattack. The lack of such a precedent only reinforces the need for caution when making analogies between cyber and kinetic actions in assessments related to *jus ad bellum*.'[101]

At the beginning of 2024, however, there has been a major development that definitively removes the argument that only a few States had a position on the relationship between cyber operations and the use of force. The formal position adopted by the African Union represents a qualitative leap of the greatest importance. In fact, more than fifty States accept that a cyber operation could trigger in the legal regime the use of force and even that of self-defence. We thus

---

[98] See Cyber Law Toolkit Project https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Real-world_examples. Also, the CENTRE FOR STRATEGIC AND INTERNATIONAL STUDIES has organized a comprehensive record of 'Significant Cyber Incidents Since 2006'. See https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. If some of them had a substantial impact on the target, there was no reference to artcile 2, 4, UN Charter or to the prohibition of the use of force in international relations. In many cases, even recent ones, the attacks are considered as criminal activities (there is mention of 'cybercriminals'). There is not a single case in which the target-State has qualified the attack as an 'aggression' or has established any parallel between the cyber operation and military actions.

[99] See NICHOLAS TSAGOURIAS AND RUSSELL BUCHAN, 'Automatic Cyber Defence and the Laws of War' (2017) 60 Ger Yearb Int Law 203–238. Automatic Cyber Defence (ACD) may include an offensive dimension, described as follows, at 205: '[o]ffensive cyber defence can include operations to retrieve, corrupt, and delete stolen data, impede further distribution of stolen data, and disable hostile email accounts, servers, networks, and computers that are responsible for hosting and distributing the attacking code'. This is also good evidence on how it would be a difficult task to apply artcile 51 (and the concept of 'classical' self-defence)to this kind of reactions.

[100] *On the Application of International Law in Cyberspace*, 6 https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf. Germany relies on the effects criteria and 'weaponizes' cyber, quoting the *Nuclear Weapons* Opinion: 'These provisions [of the UN Charter] do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons'. ICJ, 'Legality of the Threat or Use of Nuclear Weapons', Advisory Opinion, 8 July 1996, 244, par. 39. See also MARCO ROSCINI, 'Cyber Operations' 302–304.

[101] UNGA A/76/136, 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266', 13 July 2021, 19.

have a situation in which adherence to a set of common principles in cyber matters is no longer 'inter-local' in a regionalized way but takes on a true 'inter-national' dimension. It should also be noted that this is a balanced position that places respect for the sovereignty of States (as a principle of international law) and the principle of non-intervention in their due place.

Understandably, no State has ever communicated to the United Nations Security Council (UNSC) any kinetic or cyber measures adopted under the inherent right of self-defence against a cyber 'aggression', if one may use this terminology[102]. It is therefore not an easy task to conceive of a State using conventional armed force in response to a hostile cyber operation directed against it, as I suppose that in general, other States would qualify this action as disproportionate or even as an act of aggression under international law. And, although reporting to the UNSC is a procedural obligation (that, if not followed, does not jeopardize the inherent right of self-defence, as the International Court of Justice (ICJ) clearly declared in *Nicaragua*),[103] it is also not irrelevant in terms of burden of proof. As stated in *Military Activities in the Territory of Congo*, if a State fails to report to the UNSC a military action under article 51, it will reinforce the perception that the State itself was not considered to be acting under a lawful right of self-defence[104].

There is the risk of a gap between the doctrinal architecture of international law applied to cyber operations, on the one side, and the effective practice of States, on the other side. To summarize, there is a widespread opinio juris on the inclusion under certain conditions (attribution, scale and effects doctrine, international element) of cyber operations under the framework of use of force, and there are countless cases of cyber-attacks… but there is no 'practice'. Taking the two constituent elements of customary international law rules, it is necessary to 'ascertain whether there is a general practice that is accepted as law (*opinio juris*)'[105].

---

[102] With reference to UNGA resolution 3314 (XXIV), which declares that 'aggression is the most serious and dangerous form of the illegal use of force' (5th Preambular par.). In *Nicaragua*, the ICJ quotes this resolution (article 3, g)) when discussing the 'scale and effects' criteria. Also, the same conceptual proximity between armed attack and aggression can be found in ICJ, *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda)*, Merits, Judgment of 19 December 2005, 223, par. 146.

[103] ICJ, Nicaragua, par. 200.

[104] ICJ, *Case Concerning Armed Activities on the Territory of the Congo* cit., pars. 144–146. Quoting the Court (par. 145), 'in August and early September 1998 Uganda did not report to the Security Council events that it had regarded as requiring it to act in self-defence'.

[105] ILC, *Draft Conclusions on Identification of Customary International Law*, 2018, conclusion 2.

This is challenging when revisiting the Tallinn Manual. In fact, 'general practice accepted as law'[106] is not about politics, novelty, or (in)capacity to adapt. It is a formal source of positive law, subject to some clear rules.

Sooner rather than later, international lawyers must face this ambiguity, this discrepancy between the large doctrinal consensus (supported by formal declarations of States) and the different practices from States and international organizations (to say the least, it might sometimes be qualified as opposite or contradictory).

Certainly, this is a matter of degree. Almost all States that have made public their position on the main legal issues of cyberspace agree on issues such as the general application of the UN Charter and International Law, on the specific application of the *jus ad bellum* and the jus in bello, on the general principles of State responsibility, and on the protection of sovereignty[107].

It can nowadays be objectively stated that there is a theoretical consensus (at the level of the *opinion juris*) among most States on the connection between *jus ad bellum* and cyber operations. This is a major evolution, but it is simply not enough

---

[106] Article 38, ICJ Statute.

[107] I assume without further discussion that every infringement of State's sovereignty is wrongful under customary international law. It is an intriguing development, but in 2018 UK's Attorney-General, Jeremy Wright, developed a new interpretation of sovereignty, 'delegalizing' it or transforming it, at least partially, in a 'political' principle. As a logical consequence, not every interference will amount to an illegal intervention. See JEREMY WRIGHT, *Cyber and International Law in the 21st Century*, 23 May 2018: 'Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law.' It would be difficult to disagree more. Also, invoking article 2, 7, of the Charter to support the 'rule prohibiting interventions in the domestic affairs of states' does not seem legally accurate, as this article protects States against undue interventions from the Organization itself (with the obvious exceptions of measures adopted under Chapter VII), not from other States (although the prohibition is a rule of customary international law). See https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. The US publicly supported this position of the UK two years later, in 2020. See PAUL NEY, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, 2 March 2020 https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/. RUSSELL BUCHAN has rightly criticized this quite extraordinary position, 'When More is Less: The US Department of Defense's Statement on Cyberspace', EjilTalk, 30 March 2020 https://www.ejiltalk.org/when-more-is-less-the-department-of-defenses-statement-on-cyberspace/. See also, more recently, RUSSELL BUCHAN AND NICHOLAS TSAGOURIAS, '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', EjilTalk, 20 February 2024, 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/; and NICHOLAS TSAGOURIAS, 'The Legal Status of Cyberspace: Sovereignty Redux', *Research Handbook*, *supra* at 7, 19–24.

without at least some practice[108].

The dilemma is not new for international lawyers. There are several cases in which a wide agreement on a guiding general principle was undisputed but was afterwards absent in practice. This happened with two important conventional efforts that still lack relevant acceptance from States: the United Nations Conventions on the Succession of States, and the UN Convention on Jurisdictional Immunities of States. This is even more important today, a new era in which new binding instruments (such as multilateral treaties) are vanishing from international practice.

Anyway, this is a decisive momentum to define the 'times' of war and the adequacy of certain old concepts to a 'new' (or not so new) cyber reality.

2. WHAT IS 'IMMINENCE', AND DOES IT WORK IN THE CYBER CONTEXT?

As a concept, imminence challenges today's legitimacy of conventional or kinetic self-defence reactions. There is the common or literal significance of 'imminence', which implies an armed attack that almost inevitably will occur in a very near future. Let us call it the 'Six Days War criterion'[109].

In such a case, the decision to react is subject to immediate (and quite objective) scrutiny. Was the imminent threat real? Would it amount, if fully executed, to the most serious form of the use of force? This is the 'easy' application of the imminence criterion, even if it represented a significant change, considering the wording of article 51 of the Charter ('if an armed attack *occurs*'). Kofi Annan, then UN Secretary-General, confirmed it in 2005: 'Imminent threats are fully covered by Article 51, which safeguards the inherent right of sovereign States to defend themselves against armed attack.'[110] Imminent threats were opposed to the ones that were 'only' latent, in which case dealing with them (even with the authorization to use force) was an exclusive power of the UNSC[111].

---

[108] See ILC, 'Draft Conclusions on Identification of Customary International Law, with Commentaries', 2018 https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf.
[109] I assume the validity of Israel's arguments on the imminence of an armed attack against its territory. This is not something that several authors accept. See JOHN QUIGLEY, *The Six-Day War and Israeli Self-Defense, Questioning the Legal Basis for Preventive War* (CUP 2013).
[110] See *In Larger Freedom: Towards Development, Security, and Human Rights for All; Report of the Secretary-General*, UN Doc. A/59/2005 (2005), 21 March 2005, par. 124.
[111] Ibid par. 125.

Nevertheless, international reality and, consequently international law, are never so simple. Soon afterwards, this classical scenario was to be conciliated with other different 'imminences' on the use of force in other fields of international law. This contributed to the discussion on the fragmentation of international law. There is a solid trend: if the legitimacy to use force is at stake, 'imminence' is being gradually dissociated from a *temporal criterion* and even from an *identifiable threat*, therefore approaching the 'preventive' criterion unfortunately tested in Iraq in 2003, with the results known by all. It is difficult to forget the intense debate on a second resolution following the adoption of UNSC resolution 1441 to authorize the use of force against Iraq, and the serious consequences that this debate had to the institutional authority of the UNSC.

This was also the case with recent legal justifications in military actions taken against members of transnational terrorist organizations (such as Al-Qaeda and ISIS), some of them being nationals of the State, and with the killing of Soleimani, the Iranian high-ranking official leader of the Revolutionary Guard.

In its rule 73, the Tallinn Manual enshrines both verified and imminent cyber armed attacks as giving rise to the right of self-defence and adds immediacy as a further requirement[112].

Not surprisingly, the discussion on imminence goes beyond the use of military force and 'occupies' other chapters of International Law. If one applies it to climate change, environmental issues, or human rights[113], the *temporal criterion* is more restrictive, less fluid, even if the concretion of the result is not immediate. See, for instance, the position taken by the ICJ in the *Gabcíkovo-Nagymaros* case[114] and, more recently, the Human Rights Committee decision in the *Teitiota* case[115]. So, the question is: what will be the imminence criterion applicable to deciding that a State

---

[112] See TALLINN MANUAL, Rule 73, *Imminence and immediacy*: The right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy.

[113] See A. ANDERSON, M. FOSTER, H. LAMBERT AND J. MCADAM, 'Imminence in Refugee and Human Rights Law: a Misplaced Notion for International Protection' (2019) 68 ICLQ 111–140. The author rightly insists, as for the interpretation of human rights protection, the key issue is *foresseability*, not *certainty* (ibid 137).

[114] Discussing the concept of imminence under the context of environment and state of necessity, the ICJ ascertained that '"[i]mminence" is synonymous with "immediacy" or "proximity" and goes far beyond the concept of "possibility"'. ICJ, Case Concerning the *Gabcíkovo-Nagymaros Project (Hungary/Slovakia)*, Merits, Judgment of 25 September 1997, par. 54.

[115] HRC, Views adopted by the Committee under article 5 (4) of the Optional Protocol, concerning communication No. 2728/2016, I https://www.refworld.org/cases,HRC,5e26f7134.html.

is entitled to self-defence in reaction to a serious cyberattack? I have no technical capacities, and I will never have such capacities, to evaluate if a cyberattack is imminent. But I certainly know that to put into action the most serious *jus ad bellum* clause is more than a detail. It is a legal problem, but it is even more a unilateral and fundamental political decision.

Imagine a scenario where State A decides in good faith to act militarily under article 51, reacting to an imminent threat of a kinetic armed attack from State B. Take, for instance, the 1967 precedent of the Six Days War. Such a decision by State A defines State B as the wrongdoer, with all the attached consequences. Currently, many States would probably accept that State A is entitled to invoke self-defence. However, if, in a different scenario, State A decides to act in self-defence invoking an imminent 'cyber armed attack' and launches a conventional response (vg, the bombing of the secret services building of State B), what would be the overall reaction of the international community? It would certainly be different, and most States would consider that State A had unlawfully launched an armed attack against State B.

The answer could be 'This is a matter of power, not a matter for international law.' Although one may disagree, at least the argument is understandable. However, the simple assertion of the rule does not automatically ensure its existence and even less its legal validity.

I will only recall, on this issue, the March 2021 modest results of the open-ended working group on developments in the field of information and telecommunications in the context of international security, which gathered 140 States[116].

Even if we consider well-known precedents on allegations of self-defence against an imminent conventional or kinetic threat or attack, the results are not encouraging (the last example being the 'justification' of Russia to launch an armed attack against Ukraine). Lastly, if there is no precedent for the direct invocation of article 51 to legitimize a response to cyber operations similar in its effects to a conventional armed attack, there must be a reason why. An important one is

---

[116] A/AC.290/2021/CRP.2, *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report* https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf. See also UNGA, A/76/135, 14 July 2021, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement,

subjectivity. It is not an easy task to apply a generally recognizable standard to the 'gravity' of a cyberattack. On this topic, consensus among States is a hard task. There is a joke about lawyers that could also be applicable in this context: whenever you have two in a room, there will be three different legal opinions. But do not get me wrong, this is not only about lawyers and legal debate. This is also no less about common ground for political decisions.

3. A SERIOUS CYBERATTACK AND WE ARE AT WAR?

Does a cyber operation equivalent to a kinetic armed attack necessarily lead to the application of IHL? The question may seem useless if we take alleged formal law as a sacred rule. If a State launches a kinetic attack and cyber operations are an element of the ongoing process of aggression, there will be an armed conflict. This happened recently in the aggression against Ukraine, but no government alleged that the cyber operations *before* the launching of the conventional invasion marked the beginning of the conflict[117].

Interestingly, the terms used in the Tallinn Manual[118] point in this direction. Cyber operations 'in the context of an armed conflict' will be clearly regulated by IHL. Also, States generally confirm the Rule, and some recent examples support the conclusion[119].

---

[117] See, for an evaluation of cyber operations and the war on Ukraine, JAMES ANDREW LEWIS, 'Cyber War and Ukraine' CSIS https://www.csis.org/analysis/cyber-war-and-ukraine, 16 June 2022, 1–14. One of the main points is that cyber operations 'have provided little benefit': 'It may offend the cyber community to say it, but cyberattacks are overrated. While invaluable for espionage and crime, they are far from decisive in armed conflict. A pure cyberattack, as most analysts note, is inadequate to compel any but the most fragile opponent to accept defeat'. The second one is about the crucial importance of Ukrainian's preparation since 2014 and of the assistance 'in its cyber defense by friendly countries and private actors with whom it had developed cooperative relationships before the conflict. This preparation allowed it to deflect many Russian offensive cyber operations, suggesting that a well-prepared and energetic defense can have the advantage over offense in cyberspace.' On the limited role of cyberattacks during the war in Ukraine, KRISTEN E. EICHENSEHR, 'Ukraine, Cyberattacks and the Lessons for International Law' (2022) 116 AJIL 145–149. This ambiguity is not an exclusive of the current conflict in Ukraine, but it may be reinforced by the elusive strategy of the wrongdoer. See MICHAEL N. SCHMITT, *Grey Zones in the International Law of Cyberspace*, (2017) 42, 2 YJIL online 1–21 https://www.yjil.yale.edu/grey-zones-in-the-international-law-of-cyberspace/.

[118] See TALLINN MANUAL, Rule 80 (Applicability of the law of armed conflict): 'Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict.'

[119] On December 2023, 'Ukrainian state hackers crippled Russia's largest water utility plant by encrypting over 6,000 computers and deleting over 50 TB of data. Hackers claimed their attack was in retaliation for the Russian Kyivstar cyberattack', also in December 2023. CSIS, *Significant Incidents*.

The issue is different when we consider cyber operations alone. If they could amount to an armed attack and justify self-defence, it would seem logical to qualify the effects of the cyberattack as potentially involving the civilian population and thus the application of the 1949 IV Geneva Convention.

It may seem logical, but difficult to consider as a realistic possibility – there is no single example that could confirm such a proposition. Again, one faces the risk of taking legal comparison and analogy too far, and it would be legally preferable to distinguish two situations.

In the first one, *during an armed conflict* (or 'in the context of armed conflict', to use the wording of the Tallinn Manual)[120], cyber operations may amount to violations of IHL (even if this is more a theoretical legal statement than one resulting from practice). In the second situation (again, theoretically), a cyber operation could amount to an armed attack and justify a cyber response or even a conventional military response. To admit that is to accept that the two States are to apply IHL in their relations from that moment onwards (and not only human rights law). Yet, this is much more a kind of legal wishful thinking than positive international law.

Even considering the simultaneous application of international humanitarian law and international human rights law (as the ICJ stated in the *Wall Advisory Opinion*)[121], this 'Pandora's box' will not be closed so easily. In fact, the mere applicability of international human rights law to cyber activities, as enshrined in rule 34 of the Tallinn Manual[122], opens the door to the extraterritorial application of International Human Rights Law and to the debatable arguments on effective control to establish jurisdiction.

4. UNDERMINING AGENCY? A NEW INTERPRETATION OF ARTICLE 8 OF THE INTERNATIONAL LAW COMMISSION'S DRAFT ARTICLES ON STATE RESPONSIBILITY (DASR)

[120] See TALLINN MANUAL, Rule 80.
[121] 'As regards the relationship between international humanitarian law and human rights law, there are thus three possible situations: some rights may be exclusively matters of international humanitarian law; others may be exclusively matters of human rights law; yet others may be matters of both these branches of international law.' ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, par.106.
[122] Rule 34 – Applicability: International human rights law is applicable to cyber-related activities.

Attribution is a sine qua non (and the more difficult[123] element to define whether a cyber operation amounts to the use of force. The fact is that to apply the law of State responsibility and therefore international law in general, it is mandatory to 'disclose' the State. I will not elaborate on the general rules of attribution established by the International Law Commission (ILC), considering all of them international customary rules, nor on the specific technical aspects of attribution of a specific cyber operation to a State[124]. And I will not consider the position of certain States, such as the US, the UK, anda few others, that make the distinction between several forms of attribution: political, technical, and legal. That discussion goes far beyond the purpose of the present communication.

Nevertheless, as the Ukrainian conflict corroborates, the definition of legal frontiers between State and private actors[125] can be a quite challenging task. The problem is visible when the situation appears to be one in which a 'person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct', and the ongoing discussion on the *effective* control criteria (established by the ICJ in *Nicaragua*[126] and confirmed in the *Genocide* case[127]) or the global control criteria (developed by the ICTY in the *Tadic* case[128]). One should remember, for instance, that the Ukrainian Government has created a so-called 'IT army', with the identification of objectives and targets

---

[123] See MARCO ROSCINI, *Cyber Operations* 299; NICHOLAS TSAGOURIAS AND MICHAEL FARRELL, 'Cyber Attribution: Technical and Legal Approaches and Challenges' (2020) 31 EJIL 941–967.

[124] Public attribution may be more of the political than the legal sphere. See ARIEL E. LEVITE, LU CHUANYING, GEORGE PERKOVICH and FAN YANG (eds), *Managing U.S.-China Tensions Over Public Cyber Attribution* (Carnegie Endowment for International Peace, Schanghai Institutes for International Peace, Wahington/Brussels 2022), and, more specifically, ARIEL E. LEVITE AND JUNE LEE, *Attribution and Characterization of Cyber Attacks*, 33–43. See also JAKE SEPICH, *The Evolution of Cyber Attribution*, American University, 19 April 2023 www.american.edu/sis/centers/security-technology/the-evolution-of-cyber-attribution.cfm.

[125] Regarding non-state actors, the TALLINN MANUAL, Rule 17 – Attribution of cyber operations by non-State actors: 'Cyber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own.' The criteria are similar to those enshrined in articles 8 and 11, DASR.

[126] ICJ, Case Concerning *Military and Paramilitary Activities in and Against Nicaragua*, Nicaragua v. United States of America, Judgment, Merits, 27 June 1986, pars. 106–116.

[127] ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, Bosnia and Herzegovina v. Serbia and Montenegro, Judgement, Merits, 26 February 2007, pars. 400–406.

[128] ICTY, *Prosecutor v. Dusko Tadic*, IT-94-1-A, Judgement, Appeals Chamber, 15 July 1999, pars. 116–118; 120–122 and 137 https://ucr.irmct.org/scasedocs/case/IT-94-1#appealsChamberJudgement.

by the National Defence Ministry via Telegram[129]. This occurred in the context of an ongoing armed conflict, and from the news and other sources it is possible to conclude that this 'army' has been active in targeting Russian institutions, even if the results achieved are less impressive than what was anticipated[130].

What if the hostile actions of the 'IT army' were to be qualified as internationally wrongful if attributed to Ukraine? Would article 8 of the DASR be applicable? Or should they be considered as State agents, under the strict criteria defined in 2007 by the ICJ in the Genocide Case? Or could article 11 be considered in certain circumstances? Is agency, in the cyber domain, subject to adapted rules of attribution considering the specificities of the cyberspace? The position of Germany on this issue is a wise one: '[w]hile a sufficient degree or intensity of (…) control is necessary, the State is not required to have detailed insight into or influence over all particulars, especially those of a technical nature, of the cyber operation'[131] .

5. DIRECT' PARTICIPATION IN AN ARMED CONFLICT WITH OFFENSIVE CYBER OPERATIONS BELOW THE THRESHOLD OF THE USE OF FORCE)

The criteria of scale and effects have been tested in several recent situations, and particularly in the Ukrainian war. Nevertheless, if international law applies to cyber operations, this is the easy part. Significant support is possible if certain general principles are at stake, such as the protection of sovereignty, the prohibition of intervention, the protection of human rights, or the application of IHL. Conversely, difficulties arise when one tries to define legal responses to a concrete

[129] See TILMAN RODENHÄUSER AND MAURO VIGNATI, '8 Rules for "Civilian Hackers" During War, and 4 Obligations for States to Restrain Them', EjilTalk, 4 October 2023 https://www.ejiltalk.org/8-rules-for-civilian-hackers-during-war-and-4-obligations-for-states-to-restrain-them/; JENNIFER MADDOCKS, *Ukraine Symposium – State Responsibility for Non-State Actors' Conduct*, 4 Nov 2022, Articles of War https://lieber.westpoint.edu/state-responsibility-non-state-actors-conduct/; KRISTEN E. EICHENSEHR, 'Symposium on Ukraine and the International Order, Ukraine, Cyberattacks, and the Lessons for International Law' (2022) 116 AJIL unbound 14–149; STEFAN SOESANTO, 'The IT Army of Ukraine, Structure, Tasking, and Ecosystem' Cyberdefence Report, Zürich, June 2022 Center for Security Studies (CSS), ETH Zürich https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf ; and https://twitter.com/ITArmyUKR.

[130] Anticipating some of these questions and doubts, see DURWARD E. JOHNSON AND MICHAEL N. SCHMITT, 'Responding to Proxy Cyber Operations Under International Law' (2021) 6 CDR 15–34.

[131] UNGA, *Official Compendium*, 31 ff., 39–40.

situation. The statement on the application of a case-by-case analysis model[132], the ambiguity on the eventual application of article 5 NATO Treaty, and the remarkably different interpretations on the threshold that legitimizes a response under the law of self-defense, oblige one to take a less enthusiastic approach to the similarities or analogies between the kinetic and the cyber domains[133].

Invoking customary international law is simply not enough. Let us suppose that, in a very canonical situation, during an international conflict between State A (the aggressor) and State B, a third State (C) launches a series of military actions against A. To qualify this action under international law, the solution would be 'simply' applying the scale and effects criterion in a situation of kinetic action. Imagine now applying the same criterion to a specific series of offensive cyber operations launched by State C against State A, and that these actions are equivalent to a kinetic armed attack or, at least, to a situation of use of force under article 2, 4[134]. Either State C was legally acting under the umbrella of collective self-defense, or it was acting on its own initiative, without having been asked to do so by the injured State. In the first situation, at least, State C would be under the obligation to communicate this cyber operation to the UNSC. In any other case, it would be very difficult for State C to justify a hostile cyber operation, unless we consider that it was launching an attack against an aggressor (in this way).

Let us now move to an interesting episode. At the beginning of June 2022, General Paul Nakasone, the Head of the US Cyber Command on the actions of the United States (US) against Russia, declared the following in an interview to Sky

---

[132] NATO *Brussels Summit Communiqué* (2021), *supra* at 1, par. 32. There is also an acceptance of the accumulation of events criterion: "Allies recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack".

[133] SARAH WIEDEMAR, 'NATO and Article 5 in Cyberspace', CSS Analysis in Security Policy, May 2023 https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse324-EN.pdf

[134] The principle of equivalence has been accepted for approaches that would be questionable even for kinetic actions. See, vg, TERRY D. GILL and PAUL A. L. DUCHEINE, 'Anticipatory Self-Defence in the Cyber Context' (2013) 89 Int Law Stud Series, US Naval War, 438 ff. Again, the discussion is only 'possible' if from the beginning some assumptions are accepted, even if there is no State practice to support these assumptions. The authors adopt this approach. As an example of assumption, for instance, see at 439: 'there are no separate rules and legal principles for the use of force in the cyber context. Therefore, notions such as "use of force", "armed attack", "necessity", "immediacy" and "proportionality" are no different in the cyber context than in the physical world, although the modalities of their application might well differ to some extent.' Nevertheless, there is a consensus on the applicability of international law to cyber warfare. See GARY D. BROWN, 'International Law Applies to Cyber Warfare! Now What?' (2017) 46, 3 Southwest Law Rev 355–378.

News: 'We've conducted a series of operations across the full spectrum: offensive, defensive, [and] information operations.'[135]

He added that these operations were legal, without further explaining on which grounds. There are several surprising elements here. First, the US publicly admitted that they had conducted offensive cyber operations against Russia to support Ukraine. Was this a *jus ad bellum*, or rather a *jus in bello* action? Technically, it could be both, under the framework of article 51 of the Charter (collective self-defence) and within the context of an ongoing international armed conflict. Since the (formal) beginning of the conflict, the US have been very cautious in avoiding escalating the conflict. Similarly, Europeans declare that they are supporting Ukraine in its exercise of *individual* self-defense, not (formally) under the right of collective self-defense. Plausibly, the better legal definition of this 'support' is collective self-defense. Nevertheless, the purpose of insisting in the argument on *aiding* the individual exercise of self-defense is clear and understandable (or even mandatory): not to escalate the conflict.

The second surprising element in this episode is the silence of Russia, avoiding any comment in a situation in which it could (easily) have taken political advantage. The fact, I believe, is that we cannot legally compare the political and practical effects of a cyber operation with those of a conventional armed intervention in a conflict. Make no mistake, General Paul Nakasone was fully aware of what he wanted to say, and he had full political support to do so. He also knew that these actions were, for both parties, clearly below the threshold of the use of force, and therefore below the threshold that defines an armed attack. Thus, the silence of Russia was neither a surprise, nor a misinterpretation of the US actions. Furthermore, as it seems, neither States consider this sort of action to be active participation in the hostilities.

6. THE NON-INVOCATION OF IMMINENCE AS A JUSTIFICATION FOR A MASSIVE CYBER OPERATION

States have never warranted cyber operations on the grounds of an imminent threat justifying pre-emptive or preventive self-defense. On the contrary, in terms of the conventional use of force, in the last two decades we have witnessed

[135] See https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139.

all kinds of 'new' examples of adaptation to new threats involving the use of force: Afghanistan in 2001, Iraq in 2003, targeted killings, Libya and the collapse of R2P in 2011[136], Syria since 2012[137], the 'unwilling or unable' theory, etc. There is a relevant example that reinforces this perception. Between 2010 and 2012, Israel seemingly launched several cyberattacks against Iranian nuclear facilities, severely limiting its capabilities of developing a military nuclear program[138]. Iran reported in June 2010 that the Stuxnet virus had effectively 'destroyed hundreds [others say thousands] of centrifuges used to enrich uranium at the Natanz nuclear enrichment facility'. Commenting on this episode, the Cyber Law Kit stated, 'Stuxnet has been seen as the first ever cyber-attack which caused destructive effects. It opened a precedent demonstrating that cyber-weapons can be efficiently targeted against critical infrastructures not only to disable them but also causing destruction.'[139]

The involvement of Israel and the US was commonly discussed in the international realm. Both States never denied the allegations. Israel publicly and routinely declared that the Iranian nuclear program was a direct threat to its security and a potential cause for war. The Stuxnet cyberattack caused a significant blow to the Iranian nuclear program[140], similar in its effects to the *raid* against the Osiraq nuclear plant, in 1981.[141]

Understandably, neither Israel nor the US had specific interest in addressing the Security Council on this issue. Why should they? For those who insist on the principle of equivalence determined by the effects, it will be more challenging to explain the silence of Iran, as opposed to the heated debate in the UNSC after the

---

[136] See UNSC 1973, 17 March 2011 https://documents.un.org/doc/undoc/gen/n11/268/39/pdf/n1126839.pdf?token=nSrsimRYFcZ3gkHX8x&fe=true.

[137] MICHAEL N. SCHMITT AND CHRISTOPHER M. FORD, 'Assessing U.S. Justifications for Using Force in Response to Syria's Chemical Attacks: An International Law Perspective' 9 J Natl Secur Law Policy 283–303 https://jnslp.com/wp-content/uploads/2018/01/Assessing_US_Justifications_for_Using-Force_2.pdf.

[138] FRANCIS GRIMAL AND JAE SUNDARAM, 'Cyber Warfare and Autonomous Self-Defence' (2017) 4, 2 JUFIL 312–343.

[139] UNITED STATES INSTITUTE FOR PEACE, *Israeli Sabotage of Iran's Nuclear Program*, 24 April 2021, in https://iranprimer.usip.org/blog/2021/apr/12/israeli-sabotage-iran%E2%80%99s-nuclear-program).

[140] https://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/, 2010

[141] See https://www.9news.com.au/world/iran-calls-natanz-atomic-site-blackout-nuclear-terrorism/404a5a0a-8a5a-4a6f-b1d0-d1325b920baf. REESE NGUYEN, 'Navigating *Jus Ad Bellum* in the Age of Cyber Warfare' 101 Calif Law Rev 1079–1129, shows convincingly that the Stuxnet episode should have been considered as amounting to use of force under international law. However, no State has considered (at least, formally) that article 2, 4 was at stake.

Osiraq incident[142]. To be clear, there were two main consequences for Iran. The first and more obvious one was the destruction of part of its nuclear project. The second was the significant reinforcement of Iran's cyber capacities, both defensive and offensive[143]. Several years later, in 2021, a new cyberattack sabotaged the Iranian nuclear facilities of Natanz. Again, the attack was attributed to Israel. 'Natanz was knocked offline, severely hampering Iranian ambitions to develop nuclear-armed weapons.'[144]

Iran's Atomic Energy Organisation described this action as 'nuclear terrorism' and a 'terrorist action', therefore referring to the attack under an approach of criminal law much more than one that implies the concepts of use of force and aggression. The chief of the Organisation, Akbar Saleh, said that 'Iran reserves the right to respond against the perpetrators, and those who committed the terrorist action.' Almost simultaneously, several Israeli media (among them, Kan, public broadcaster) reported that Israel was behind this attack. So, there are no special doubts on: a) who 'did' it; b) the consequences and damaging effects of this attack; and c) the silence on including these events under an article 2,4 focus[145].

7. INDIVIDUAL COUNTERMEASURES AND PLURAL (COLLECTIVE) MEASURES?

To conceive of tit-for-tat countermeasures is always a hard task. In general terms, State responsibility establishes two major categories of countermeasures and other 'measures' as responsive actions that target the State author of the international wrongful act: (a) the injured State[146], and (b) other States that are not

---

[142] See REESE NGUYEN, 'Navigating *Jus Ad Bellum*' 1082–1083: 'In effect, Stuxnet produced physical damage of the Iranian nuclear facility comparable to that caused by the 1981 and 2007 Israeli air strikes that destroyed partially constructed nuclear reactors in Baghdad and Syria' (footnotes omitted); STEVEN E. LOBELL, 'Why Israel launched a preventive military strike on Iraq's nuclear weapons program (1981): The fungibility of power resources', 46 Journal of Strategic Studies, 2023, 319-344; ANTHONY D'AMATO, 'Israel's Air Strike Against the Osiraq Reactor: a Retrospective', (1996) 10 Temp Int'l & Comp LJ 259; and LOUIS RENE BERES & YOASH TSIDDON-CHATTO, 'Reconsidering Israel's Destruction of Iraq's Osiraq Nuclear Reactor' (1995) 9 Temp Int'l & Comp LJ 437.

[143] See ADAM SEGAL, 'Cyber Conflict After Stuxnet' https://www.cfr.org/blog/cyber-conflict-after-stuxnet; and DAN EFRONY AND YUVAL SHANY, 'A Rule Book on the Shelf' 598–599.

[144] See https://www.9news.com.au/world/how-stuxnet-cyberattack-took-out-natanz-nuclear-facility-in-iran/37694f90-c2e1-454c-9597-e7de8f54e495.

[145] Also, many experts agree that this cyberattack could amount to a use of force in international law. But they also agree that it is impossible to give it as an example of a 'practice' that reinforces the general *opinion juris*. See DAN EFRONY AND YUVAL SHANY, *A Rule Book on the Shelf* 591, 620.

[146] Articles 42 and 49–53 DASR.

injured States but may nevertheless invoke responsibility and adopt 'measures'[147]. From the beginning, there is a basic assumption. There cannot be forcible countermeasures[148], as opposed to armed reprisals (now theoretically outlawed[149]). So, all countermeasures that involve the threat or use of force are illegal under international law. The ICJ was clear on this point on the *Nicaragua* case on the use of force, as in the very restrictive approach on the intervention by way of countermeasures by third States[150].

Next, the codifying efforts on State responsibility insist on other limits to the adoption of countermeasures by the injured State itself: they cannot involve the violation of human rights, military reprisals prohibited by international humanitarian law, and other obligations under peremptory norms of general international law[151]. The normative intention is, I believe, transparent.

Countermeasures can be accepted as an exceptional solution, not as an automatic reaction, and 'permissibility of third-party countermeasures remains one of the most controversial topics in the law of state responsibility'[152].

As for other arguments, it is difficult to accept the possibility of countermeasures by third States because the injured State may have defensive capacities against hostile cyber operations, but no offensive capacity to launch a response. Being realistic, the world would be much more secure and peaceful if every State had defensive capacities, even if only defensive capacities, against conventional attacks launched by another State. The fact that a State has the

---

147 Articles 48 and 54 DASR.

148 See article 50, par. 1, a), DASR.

149 The prohibition of armed reprisals (included in the more general principle forbidding the threat or use of force) gave the floor to a more 'neutral' concept of countermeasures. See UNGA resol. 2625 / XXV), 24 October 1970, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, 'States have a duty to refrain from acts of reprisal involving the use of force.' Considering that resol. 2625 expresses customary international law, ICJ, *Nicaragua* pars. 188 and 191.

150 See ICJ, *Nicaragua* par. 249: '[o]n the legal level the Court cannot regard response to an intervention by Nicaragua as such a justification. While an armed attack would give rise to an entitlement to collective self-defence, a use of force of a lesser degree of gravity cannot (…) produce any entitlement to take collective counter-measures involving the use of force. The acts of which Nicaragua is accused, even assuming them to have been established and imputable to that State, could only have justified proportionate counter-measures on the part of the State which had been the victim of these acts, namely El Salvador, Honduras or Costa Rica. They could not justify counter-measures taken by a third State, the United States, and particularly could not justify intervention involving the use of force.'

151 Article 50 DASR.

152 AMANDA BILLS, 'The Relationship between Third-party Countermeasures and the Security Council's Chapter VII Powers: Enforcing Obligations *erga omnes* in International Law', (2020) 89 Nordic J Int L,- 117-141.

capacity to neutralize the effects of every cyber operation by a wrongdoing State is, by itself, an excellent result. To consider that this is a legal justification to enlarge the legitimacy of countermeasures adopted by third States (far beyond what is acceptable in a non-cyber context) has therefore no basis in law, nor in practice.

On the one hand, as for 'measures' adopted by third States under articles 48 and 54, the approach is even more restrictive, and the result was the very strange article 54 of the ILC DASR. Third States, very plainly, are not allowed to adopt 'countermeasures', only 'measures'. This may seem a legal technicality, and indeed it is. However, it touches a fundamental point. For third States, there is no circumstance precluding wrongfulness that can justify their measures, because they are not injured States. From this perspective, their reactions must be autonomously 'lawful', *even if this conclusion is only achievable on a case-to-case basis*. On the other hand, those 'measures' should not be taken by their face value; they are not equivalent to acts of retorsion. Indeed, it would be absurd to believe that ILC decided in article 54 to 'authorize' States to adopt lawful reactions per se. Differently, in what was considered clearly as a development of international law (more than a mere codification), article 54 allowed States to design the limits of this solution, which goes far beyond a limited bilateral approach of State responsibility. It is important to insist on this point: countermeasures are not authorized per se, even if they are not explicitly forbidden *in casu*. Therefore, they are by their nature forbidden, except if they can be tolerated because of an international wrongful act that defines which is the injured State. Once this definition is made, only the injured State is legitimized to react.

The Russian Federation has been the target of an unparalleled set of so-called 'sanctions' since the armed attack launched against Ukraine in February 2022. The fact is that these measures should not be qualified as 'sanctions', as there is no formal decision of the Security Council on this issue under UN Chapter VII (unless one believes in 'moral majorities').

Among those 'sanctions', many should be considered as legal acts of retorsion, even if they are hostile or unfriendly measures. Others, such as the freezing of State or individual (the so-called oligarchs') assets, would be considered in 'normal' circumstances as international wrongful acts – unless we place them under the legal framework of collective self-defence – which I believe they are. Apparently, in the context of the Russian aggression, I dare to say that a significant part of the international community tolerates these measures.

But are they legal if we place them outside the umbrella of collective self-defence? They are certainly not 'countermeasures'. They may possibly be qualified as 'measures' adopted by third States (article 54 ILC DASR), whether individually or in execution of an institutional decision by the European Union[153]. Consequently, it is the specific context and gravity of the Russian aggression and the global agreement on this topic (see, e.g. the General Assembly resolutions condemning the Russian aggression) that make these measures not unlawful (which, in my opinion, is different from lawful), without any creation of a precedent[154].

As of 2017, there has not been an agreement on the entitlement of third States to adopt cyber countermeasures (or, more precisely, 'measures') to 'ensure cessation of the breach' – in the situation of a 'breach of an international obligation by an act of a State having a continuing character' – and 'reparation in the interest of the injured State' (articles 54 and 14, 2, ILC DASR).

Michael Schmitt and Sean Watts have recently supported the lawfulness of 'collective cyber countermeasures', at least under certain circumstances[155]. For this purpose, they mention a 'collectivist' approach, as opposed to the 'bilateralist' approach of certain States, such as France. Indeed, France explicitly contests the possibility of third States' (not injured States) carrying out 'cyber countermeasures'.

One thing is certain. The debate on these kinds of plural 'measures' of reaction (I prefer this terminology)[156] only makes sense if the injured State and other States are reacting against hostile cyber operations that *do not amount* to the threshold of an armed attack or even to the use of force. If that were the case, the normative framework would either be collective self-defence, or measures taken under article 54. Even if third States adopt cyber measures that do not amount to an act of kinetic use of force against an aggressor, they are entitled to do so, even if they do not invoke, for instance, article 51 of the Charter, or article 5 of the NATO Treaty. This was the case with the United States' offensive cyber operations against Russia.

---

[153] Article 215, Treaty on the Functioning of the European Union, pars 1 (restrictive measures against third countries) and 2 (restrictive measures adopted against 'natural or legal persons and groups or non-State entities: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

[154] As for the TALLINN MANUAL 2.0, '[o]nly an injured State may engage in countermeasures, whether cyber in nature or not' (rule 24) and '[c]ountermeasures, whether cyber in nature or not, must be proportionate to the injury to which they respond' (rule 23).

[155] MICHAEL SCHMITT and SEAN WATTS, 'Collective Cyber Countermeasures?' (2021) 12 NSJ 373–411.

[156] The fact is that there is no collective decision, and the support given to the State has no institutional ground. Therefore, *any* decision remains *unilateral*, even if coordinated among several States.

Next, the 'measures' are only admissible when the strict conditions of article 48 are met, not to mention the many other conditions and limits defined in articles 49 and 50 DASR. This said, the 'conflict' between the 'bilateralists' and 'collectivists' (it is interesting to notice the quite 'ideological' choice of 'collectivist' to describe collective measures) is more apparent than real. The positions taken by France and Estonia on this topic are not radically opposed. Even if it was the case, it is important to stress that the more recent position of Estonia (in 2021) omits any reference to collective countermeasures except in the case of 'injured States'[157].

As for other States, there is a broad agreement on restricting the adoption of countermeasures to the injured State. See, for instance, Australia[158]; Brazil, stating that the ILC provisions on countermeasures 'went beyond the codification of customary norms and had a strong element of progressive development of international law' and that several States criticized countermeasures 'because they would be prone to abuses, especially due to the material inequality of States'[159]; Germany[160]; Japan ('a State that has been injured by an international wrongful act of another State may take, under certain conditions, countermeasures')[161]; the Netherlands[162] ('[i]f a state is the victim of a violation by another state of an obligation under international law (…) it may under certain circumstances take countermeasures in response'); Norway (only the injured state)[163]; Romania[164] ('the injured(s) State(s) may recourse to countermeasures'); the Russian Federation[165]; Singapore[166]; Switzerland[167] ('the injured state(s) may also take countermeasures in the form of reprisals, provided that the applicable rules governing state responsibility are observed'); the UK[168]; and the United States[169].

---

[157] On the 2019 declaration of Estonia, commenting a speech of the then President of this country at the CyCon 2019, see M. SCHMITT, 'Estonia Speaks out on Key Rules for Cyberspace' in https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/.
[158] UNGA *Official Compendium* 3 ff., 8.
[159] Ibid 17 ff., 21.
[160] Ibid 31 ff., 41.
[161] Ibid 44 ff., 48.
[162] Ibid 54 ff., 62.
[163] Ibid 65 ff., 72.
[164] Ibid 75 ff., 79.
[165] Ibid 79 ff., 80.
[166] Ibid 83 ff., 84.
[167] Ibid 85 ff., 90
[168] Ibid 115 ff., 118.
[169] Ibid 136 ff., 142.

One should note that in 2022 the UK launched a debate considering, for the first time, a different possibility: '[h]owever, some countries simply do not have the capability to respond effectively by themselves in the face of hostile and unlawful cyber intrusions. It is open to States to consider how the international law framework accommodates, or could accommodate, calls by an injured State for assistance in responding collectively.'[170]

There are convincing legal arguments opposed to such a possibility. The same differences on reactive capacity exist as for non-cyber countermeasures, and the possibility of third States 'assisting' the injured State in this situation has never been presented by any State, at least invoking rules of international law. All 'measures' that the ILC mentions as possible examples to interpret article 54 of the ILC DASR are non-military measures, which do not amount to a theoretical infringement of article 2, 4 of the Charter. All of them were 'validated', in a quite exceptional context (and certainly not as a new standard), to face certain international wrongful acts, without creating a general material rule of 'authorization'. It is therefore difficult to exclude some plural responsive cyber measures if we consider that other non-cyber measures can be adopted 'against' a State under article 54 ILC DASR if they do not amount to a use of force and even if they are of a higher gravity. Also, as it is understood, if the Tallinn Manual is to apply and adapt several international legal regimes (such as the rules on the use of force, IHL, or international State responsibility), it would be surprising and quite innovative (to say the least) to accept collective countermeasures from non-injured States when this solution to non-cyber peaceful reactions has been explicitly barred by the ILC. In addition, it is difficult to block third States (non-injured States in the sense of article 42 but integrating the categories of article 48) from adopting cyber 'measures' in a context in which, in general, they could be accepted by the international community, considering a specific context.

Attention should also be drawn to the following. If one of the fundamental principles of international law is the sovereign equality of States, it is by no means equivalent to any 'right' or even expectation regarding equal capacities or wealth of international subjects. The equality of States is measured by their common submission to international law. It would, therefore, be legally strange if the developing norms applicable to cyber operations were, even with little normative

[170] See https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_United_Kingd om_(2022)#citeote-6.

consolidation, contrary to the customary rules on the international responsibility of States. Brazil's position, referenced three paragraphs earlier, seems an accurate description of the actual standard of international practice. The adoption of countermeasures presupposes both the legal status of an injured State (1) and, on a level that is no longer legal, (2) the factual power to be able to adopt these countermeasures. In other words, no matter how much the topic is avoided in the legal discourse, only the most powerful States can exercise this power with a view, through a 'cost' imposed on the wrongdoer, to inducing it to the cessation of the international wrongful act, reparation, and, eventually, to provide guarantees of non-repetition[171].

Supporting the adoption of 'collective' countermeasures (limited to the cyber context) is also not convincing on additional grounds. On the one hand, inevitably, the solution would reinforce inequalities, double standards, and an escalation of tensions without visible benefits for peace and security. On the other hand, even small States have far more defensive capacities on cyber threats than on conventional ones. The level of effort (financial, political, and technological) to achieve strong cyber defence capacities is not comparable to the one needed to achieve the same protection against conventional threats.

In addition, effective defensive capacities, in the cyber or any conventional domain, are the cornerstone of the system architecture. If a State can prevent any hostile threat or attack coming from an adversary or even enemy, it achieves the fundamental goal of avoiding the damaging effects resulting from aggression. The adoption of 'collective' countermeasures is therefore even more difficult to explain when there is no damage or risk to respond to or to avoid.

8. SOME CONCLUDING REMARKS

All international lawyers, the military, and politicians are awaiting with the highest of expectations and curiosity the 3.0 version of the Tallinn Manual.

It is important to underline that its first version is more than ten years old; the 2.0 version was welcomed in 2017 and, in 2021, the NATO Cooperative Cyber Defence Centre of Excellence launched the Tallinn Manual 3.0 Project, expected to be a five-year venture.

[171] See article 30 DASR.

This will be important for an in-depth analysis of State practice in the cyber domain. The analogies and parallels with the applicable regimes to the use of 'conventional' or 'kinetic' military force, need to be confronted with the actual practice of States.

On the one hand, in general terms, both States and international organizations accept that the cyber domain is an operational domain. Furthermore, as such, it is regulated by international law. The Tallinn Manual (1.0 and 2.0) has played, plays, and will continue to play, with its next 3.0 version, a remarkable role in making this clearly established, discussed, and widely understood. However, we are witnessing the formation of certain customary rules specifically applicable to the cyber domain that are distant from being applicable to the conventional use of military force in other operational domains. Maybe the time has come to gradually accept the necessity of a more precise approach that does not necessarily take for granted the legal identity of solutions for kinetic and cyber actions, acknowledging the limits of the 'as if'. Just to give an example, the 'scale and effects' criterion is so overpowering in the political and legal debate that it literally blocks a more in-depth analysis of the real legal impact of hostile cyber operations on the principle of non-intervention and on the rule of non-interference in internal affairs, as they should be interpreted contemporaneously.

On the other hand, a certain level of grey fog involves, by its own nature, the cyber domain. Firstly, there are very distinct levels of cyber capacities amongst States and non-State actors[172]. The differences between the cyber capacities of different States are relevant, although less obvious than the differences between the conventional military capacities of States; several non-State actors (enterprises, but also, at a more inorganic level, individual hackers, or associations of hackers) are much more capable than, I would say, many States.

In fact, the impact of power in international relations and the way they influence the development of law are 'openly' present and are inherent to the cyber domain.

But it goes further. Two of the features in the cyber domain that are clearly used as conscious advantages are ambiguity and disguise. One needs just to recall the difficulties on attribution. States resist publicly accepting having been

[172] See MICHAEL SCHMITT and SEAN WATTS, 'Beyond State-Centrism: International Law and Non-state Actors in Cyberspace' (2016) 21 JCSL 595–611.

targeted by a serious cyberattack, as it reveals their weaknesses. States proclaim, in international *fora*, organizations, and official documents, the possibility of a cyberattack being an armed attack on a case-by-case analysis. However, they do not qualify concrete cyber operations that they themselves launch under a clear legal framework.

The dynamic on the identification of customary international law is challenging. In fact, the ILC's draft conclusions on the identification of customary international law state that, although customary law is a spontaneous source of international law, States need to adopt general practices linked to *opinio iuris*. And most of the time, *opinio juris* and the reasons, grounds, and legal justifications of the practice need to be defined with a minimum of clarity.

Finally, I consider that revisiting the Tallinn Manual will call for reflection on the frontiers with some of the technological weaponry development, such as autonomous weapons or machine learning in weaponry or in military decisions.

If the chance to confront and evaluate actual State practice is not taken, there is the risk of a continuing dystopia that might even undermine the application of general international legal regimes, such as the ones of *jus ad bellum*, *jus in bello*, and State responsibility in the more traditional uses of military force and 'conventional' domains. This may seem legally old-fashioned, but it would probably be preferable to develop a clearer set of rules on the solid relation between malicious cyberattacks and the principle of non-intervention, then to elaborate almost exclusively on the 'mandatory' applicability of *jus ad bellum*. Or, as the old proverb says, a bird in the hand is worth two in the bus all international lawyers, the military, and politicians are awaiting with the highest of expectations and curiosity the 3.0 version of the Tallinn Manual.

It is important to underline that its first version is more than ten years old; the 2.0 version was welcomed in 2017 and, in 2021, the NATO Cooperative Cyber Defence Centre of Excellence launched the Tallinn Manual 3.0 Project, expected to be a five-year venture.

This will be important for an in-depth analysis of State practice in the cyber domain. The analogies and parallels with the applicable regimes to the use of 'conventional' or 'kinetic' military force, need to be confronted with the actual practice of States.

On the one hand, in general terms, both States and international organizations accept that the cyber domain is an operational domain. Furthermore,

as such, it is regulated by international law. The Tallinn Manual (1.0 and 2.0) has played, plays, and will continue to play, with its next 3.0 version, a remarkable role in making this clearly established, discussed, and widely understood. However, we are witnessing the formation of certain customary rules specifically applicable to the cyber domain that are distant from being applicable to the conventional use of military force in other operational domains. Maybe the time has come to gradually accept the necessity of a more precise approach that does not necessarily take for granted the legal identity of solutions for kinetic and cyber actions, acknowledging the limits of the 'as if'. Just to give an example, the 'scale and effects' criterion is so overpowering in the political and legal debate that it literally blocks a more in-depth analysis of the real legal impact of hostile cyber operations on the principle of non-intervention and on the rule of non-interference in internal affairs, as they should be interpreted contemporaneously.

On the other hand, a certain level of grey fog involves, by its own nature, the cyber domain. Firstly, there are very distinct levels of cyber capacities amongst States and non-State actors.82 The differences between the cyber capacities of different States are relevant, although less obvious than the differences between the conventional military capacities of States; several non-State actors (enterprises, but also, at a more inorganic level, individual hackers, or associations of hackers) are much more capable than, I would say, many States. In fact, the impact of power in international relations and the way they influence the development of law are 'openly' present and are inherent to the cyber domain.

But it goes further. Two of the features in the cyber domain that are clearly used as conscious advantages are ambiguity and disguise. One needs just to recall the difficulties on attribution. States resist publicly accepting having been targeted by a serious cyberattack, as it reveals their weaknesses. States proclaim, in international fora, organizations, and official documents, the possibility of a cyberattack being an armed attack on a case-by-case analysis. However, they do not qualify concrete cyber operations that they themselves launch under a clear legal framework.

The dynamic on the identification of customary international law is challenging. In fact, the ILC's draft conclusions on the identification of customary international law state that, although customary law is a spontaneous source of international law, States need to adopt general practices linked to opinio iuris. And most of the time, opinio juris and the reasons, grounds, and legal justifications of the practice need to be defined with a minimum of clarity.

Finally, I consider that revisiting the Tallinn Manual will call for reflection on the frontiers with some of the technological weaponry development, such as autonomous weapons or machine learning in weaponry or in military decisions.

If the chance to confront and evaluate actual State practice is not taken, there is the risk of a continuing dystopia that might even undermine the application of general international legal regimes, such as the ones of *jus ad bellum*, *jus in bello*, and State responsibility in the more traditional uses of military force and 'conventional' domains. This may seem legally old-fashioned, but it would probably be preferable to develop a clearer set of rules on the solid relation between malicious cyberattacks and the principle of non-intervention, than to elaborate almost exclusively on the 'mandatory' applicability of *jus ad bellum*. Or, as the old proverb says, 'a bird in the hand is worth two in the bush'.

INTERNATIONAL SUPPORT TO UKRAINE IN CYBERSPACE IN THE UKRAINE-RUSSIA CONFLICT

Helder Fialho de Jesus
Navy Captain from the Portuguese Navy
jesus.hmf@ium.pt

ABSTRACT

The Russian Federation's invasion of Ukraine on 24 February 2022 has changed our vision of the World. A war in the European continent was unexpected, although it brought back some memories from the Balkans, and the actual conflict is not unacceptable in accordance with International Law. With the advancement of technological development, namely in the cyberspace environment, the way society depends on these technologies and the way of conducting war, in itself, has also changed. This document intends to provide some information and reflections on the International Support to Ukraine in Cyberspace, as it is an essential part of this conflict. This support can be direct or indirect and has several natures, from technical aid to capability development or to financial assistance, amongst others. It can be provided by nations, international organisations or even by private companies, and the latter provide a new and different approach to this war and future wars, where the Artificial Neural Networks are an example to make intelligent decisions with limited human intervention. Digital technology is, therefore, playing a vital role in the current war between Russia and Ukraine with the "Civilianization" and the "Privatization" of the war. And it may also be defining the future of geopolitics where a possible new approach to the Revolution in Military Affairs is underway.

1. CONTEXT

To understand the cyberspace domain of this conflict, it is essential to understand the political dimension. Ukraine's main foreign policy dilemma has always been finding the correct balance between relations with the West and its relations with Russia[173], until 2014. Since this date, with the modification of the political environment in Ukraine, the United States of America (USA) has assumed a more significant role. Senior members of the Obama administration, notablyVice President Biden, frequently travelled to Ukraine. The USA heavily influenced the

[173] https://www.brookings.edu/blog/up-front/2014/02/28/ukraines-perpetual-east-west-balancing-act/

International Monetary Fund (IMF) program for Ukraine, and Washington's direct financial support has sped up several significant reforms in the country[174]. Note the article of William Taylor, who served as interim US Ambassador to Ukraine in 2019, where he significantly increased the prominence of the country, stating, "Ukraine is defending itself and the West against Russian attack. If Ukraine succeeds, we succeed. The relationship between the United States and Ukraine is key to our national security..."[175]. Indeed, since 2014, the USA and other North Atlantic Treaty Organisation (NATO) allies have participated in multinational exercises with Ukraine[176]. Thanks to Washington's persistent will, Ukrainian troops can now participate in NATO military exercises and bilateral drills with American units[177]. As an example, in cyberspace and since 2017[178], the participation of Ukrainian military experts in the Tide Hackathons and Tide Sprints series and in the NATO Multinational Training exercise "CWIX" (Coalition Warrior Interoperability Exercise), the main exercise on interoperability, hosted by the NATO Joint Force Training Centre (JFTC), located in Bydgoszcz, Poland[179].

To realize the "value" of the parts in the conflict in the cyberspace domain, it is important to analyze their capabilities, considering trustful indexes. One of them is the Global Cybersecurity Index (GCI)[180], released by the International Telecommunication Union (ITU), the United Nations (UN) specialized agency for *Information and Communications Technology* (ICT). This source evaluates countries' cybersecurity commitment toward a secure digital ecosystem. It is based on five pillars at the legal, technical, organizational, capacity building, and cooperation levels aggregated into a final rating. During its most recent edition in 2022, referencing data from 2020, the report placed the USA in the top position, Russia in fifth, and Ukraine as the 78th country due to its underdeveloped capacity development pillar. Both countries are committed to the United Nations' cyberspace initiatives, and one of the last was the approval of the final report of the Open-ended Working Group on Information and Communications Technologies

---

[174] https://www.razomforukraine.org/projects/policyreport/overview-of-u-s-policy-on-ukraine/
[175] https://www.nytimes.com/2020/01/26/opinion/Pompeo-ukraine-taylor.html
[176] https://www.bbc.com/news/world-europe-29204505
[177] https://www.armytimes.com/2020/09/14/rapid-trident-20-exercise-kicks-off-in-ukraine-with-fewer-us-troops-than-last-year/
[178] https://mil.in.ua/en/news/ukraine-unveiled-its-own-delta-situational-awareness-system/
[179] https://www.encouncil.org/wp-content/uploads/2019/10/ENG-Ukraine-EU-NATO-cooperation-to-counter-hybrid-threats-in-cyber-sphere.pdf
[180] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

(OEWG)[181], in March 2021. This group has served as a forum for United Nations member states to talk about cyberspace usage, regulation, and governance.

Harvard Kennedy School Belfer Centre for Science and International Affairs provides a different view of national cyber capabilities with the National Cyber Power Index 2022[182]. Here, a whole-of-nation approach is considered for a state's cyber power where destructive operations, espionage, or enhancing its cyber resilience is noted, "but also other state's efforts at surveillance, information control, technology competition, financial motivations, and shaping what is acceptable and possible through norms and standards". In this context, the differences between the two nations are less noticeable because Russia is ranked third while Ukraine is ranked twelfth.

Ukrainian Cyberspace has been studied in several areas of activity, namely in the academic and political environments, with some documents published. In this regard, and to help to understand the Ukrainian context, three can be noted in the present paper:

(i) "The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments"[183] (2017), where the author makes an effort to explain how cybersecurity is viewed, as well as its distinguishing characteristics, the fundamental principles guiding its delivery, the system of actors engaged, the general thrust of sectoral policies, and the specific steps they took. He concluded that four fundamental pillars make up the system of actors responsible for Ukraine's cybersecurity: defence and (counter)intelligence structures, law enforcement agencies, technical protection regulators, the private sector, and a coordinator - the National Coordination Center of Cybersecurity of the Council of National Security and Defence. Ukraine has passed several laws intended to establish a basic normative framework and control certain facets of cybersecurity. Ukraine has outlined future policy actions, identified risks to the national interests in this area of national security, and organized a group of individuals responsible for providing cybersecurity.

(ii) "Hotspot Analysis: Cyber and Information Warfare in the Ukrainian conflict"[184] (2018). Understanding the framework in which the Ukrainian war

---

[181] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
[182] https://www.belfercenter.org/publication/national-cyber-power-index-2022
[183] https://link.springer.com/article/10.1007/s41125-017-0020-x
[184] https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf

developed requires knowledge of both the historical background and the conflict's timeline. When the Soviet Union fell, Ukraine obtained its independence, but Russia continued to attempt to exert some control or influence over the former Soviet Republics. Three types of attacks can be identified in the conflict between Ukraine and Russia: DDoS13 attacks, website defacement, and spear phishing-infected malware. The latter is more strongly focused on cyber-espionage for intelligence gathering and battlefield preparation for more kinetic offensives or cyberattacks, while the previous two instruments are more appropriately classified as cyber-disruption techniques. Although there were many cyberattack victims, most were in Russia and Ukraine. This analysis divides victims into four groups according to their activity and country of origin: third parties, Russian groups, Ukrainian institutions, and Ukrainian media outlets. It examines the many internal and international repercussions of the Ukrainian conflict's cyber dimension while highlighting specific policy ramifications. The research examines the harm done to society by cyber-activities within the context of the domestic conflict in Ukraine. It also focuses on the financial consequences of such cyberattacks for businesses and governmental organizations. It looks at how the conflict's effects on technology and how those effects also led to new developments. The international implications of the cyberattacks and the western collaboration supporting the crisis in Ukraine are also noted.

(iii) "Defending the EU Against Cyber Operations-Mechanisms, Challenges and Cooperation with NATO"[185] (2021), where two of the most severe occurrences to date are presented as case studies of Russian cyberattacks and briefly discussed - the Russian cyberattacks on Estonia and Ukraine. Regarding the latter, it was stated the relations of this country with the Kremlin started to worsen in 2014, which led to the annexation of Crimea. Since then, the nation has regularly seen cyberattacks, and Russia has been using them to amplify its impact and geopolitical strength. At the same time, Ukraine appears to have become a test site for Russian adversaries to deploy their newly developed cyberweapons. Examples are given, including the Central Election Commission (CEC) hack in which the electoral networks were compromised four days before the announcement of the results of the presidential election in May 2014. On December 23, 2015, over 220,000 Ukrainians lost power

[185] https://finabel.org/wp-content/uploads/2021/11/34.-Defending-The-Eu-Against-Cyber-Operations-Mechanisms-Challenges-And-Cooperation-With-Nato-1.pdf (EU - European Union)

due to the power grid breach, which was carried out by Sandworm, a group with ties to the Russian government. Launching this kind of action on a nation's vital infrastructure takes a lot of planning. Not Petya described by the American administration as the "most destructive and expensive cyber-attack in history". Although Ukraine was the target of the attack, it affected computers worldwide. Companies, including the British advertising agency WPP, the Danish shipping and energy company Maersk, and the American pharmaceutical company Merck were all impacted. In the end, the cyberattack caused $10 billion[186] in damage worldwide and Maersk almost lost $300 million income. The results emphasize that strengthening cooperation between States and international organizations and collective cybersecurity are priorities. Prior crises, such as those discussed in this paper, have demonstrated how essential collaboration is in order to develop a complete strategy for battling digital dangers.

Several reports and books have also been written about the Russian view and behaviour in Cyberspace. As a generic view, it is possible to address two different lines:

(i) An external, with two aims:

(a) the Western public and decision makers are the focus, with Russia's interference in USA[187] and European elections[188],[189], hacking and leaking these countries as a persistent threat; and,

(b) cyberattacks on critical infrastructures, as it happened with Colonial Pipeline[190], or on supply-chain companies, with SolarWinds[191], as examples.

(ii) An internal, where is it possible to see Russia's efforts to ensure independence from the global Internet network as a new step toward the

---

[186] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[187] https://www.intelligence.senate.gov/press/senate-intel-committee-releases-unclassified-1st-installment-russia-report-updated

[188] https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

[189] https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf

[190] https://www2.deloitte.com/us/en/pages/risk/articles/is-your-critical-infrastructure-resilient-against-cyber-threats.html

[191] https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

"*splinternet*"[192], to improve their information security.

Also, to note is how Russia uses cyber operations and other military and non-military tactics to achieve strategic goals. Russia sees cyber operations as an increasingly significant tool in what it perceives as the ongoing "information confrontation"[193]. The NATO STRATCOM COE23 states that Russia considers cyberspace a tool operating within a broad definition of the information domain that includes both the technical and psychological components. Therefore, due to the interdependency of our society, we can say that cyberoperations have a direct impact on the instruments of National Power, well known as Diplomatic, Informational, Military, and Economic (DIME) on the basis, with new approaches to the Financial, Intelligence, Legal and Law Enforcement dimensions as presented by Craig Nation[194].

Cyberspace security is also an European concern, and the EU Cybersecurity Agency25 regularly provides important reports annually on the status of the cybersecurity threat landscape. It identifies the significant threats and trends, threat actors and attack techniques, their impacts, and an analysis of possible motivations. In its last edition, the tenth[195], the Russia-Ukraine conflict was naturally considered. In the context of this document, it is to note some ideas: the Impact of geopolitics on the cybersecurity threat landscape - observing that the conflict between Russia-Ukraine has reshaped the threat landscape, where Geopolitics continues to have a more substantial impact on cyber operations. Important to notice that the activities of state actors frequently include destructive attacks and the rising of hacktivism. Concerning cyberwarfare, disinformation is being used as a tool and as a threat technique, ransomware being at the top of the actions, with DDoS getting more extensive and more complex and heading to mobile networks and to Internet of Things (IoT) devices and cyber actors conducted operations in concert with kinetic military actions.

The process of socioeconomic and technological processes going digital

---

[192] https://law.stanford.edu/publications/the-splinternet/
Mark A. Lemley, The Splinternet, 70 Duke Law Journal 1397 (2021) (see also the 2020 David L. Lange Lecture on Intellectual Property by the author, also titled "The Splinternet," at: *https://scholarship.law.duke.edu/lange/4/)*.
[193] https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210
[194] https://www.jstor.org/stable/resrep12116.14
National Power_ Theory of War and Strategy_ R. Craig Nation (2012)
[195] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

in Russia is a representation of the world economy's objective patterns of development. Russia has a Strategy for the Development of the Information Society in the Russian Federation until 2030 and the National programme "Digital Economy of the Russian Federation" from up to 2024[196]. But numerous issues prevent the Russian economy and business from going fully digital, namely - social (lack of qualified personnel, etc.), economic (high cost of digital transformation), regulatory (lack of standards in the field of digital technologies), and technical (security problems, etc.)[197]. Nevertheless, digital transformation offers real opportunities to boost business growth and labour productivity.

But with this War, many tech companies, including Google, Sony, Microsoft, PayPal, IBM, CISCO (…), took a stance on the Ukraine conflict and left Russia. An increasing number of electronic companies, including chipmakers, video game publishers, and social networking heavyweights, have stopped doing business with Russia[198]. About 100,000 IT professionals, or 10% of the country's tech employment, left in 2022; however, this number is probably underestimated. Since the start of the conflict, more than 1,000 enterprises have declared their exit from Russia, according to a count by Professor Jeffrey Sonnenfeld and his research group at the Yale Chief Executive Leadership Institute[199].

This change in the technology environment in Russia shows how important artificial intelligence (AI) is. An artificial neural network (ANN)[200] in information technology (IT) is an artificial intelligence method that teaches computers to process data in a way inspired by the human brain. ANNs, often known as neural networks, are a type of deep learning technology included in the AI category. Computers can make intelligent decisions with minimal human intervention thanks to neural networks. They can learn and model complex, nonlinear input and output data relationships[201]. The technology giants across industries have made significant investments in implementing AI for their advantage, as well as many small and medium-sized firms. In fact, if AI were to be removed from their

[196] https://iopscience.iop.org/article/10.1088/1755-1315/650/1/012017/pdf
[197] https://www.europeanproceedings.com/article/10.15405/epsbs.2021.04.02.49
[198] https://www.technologyreview.com/2023/04/04/1070352/ukraine-war-russia-tech-industry-yandex-skolkovo/
[199] https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain
[200] https://www.techtarget.com/searchenterpriseai/definition/neural-network
[201] https://aws.amazon.com/what-is/neural-network/

corporate processes, their profitability would fall off immediately. This dependence highlights how quickly, and dramatically artificial intelligence technology is developing. Google, Amazon, and Microsoft are three of the major tech companies now making waves with their visions for artificial intelligence[202], in a race to create the finest AI tools, which is currently one of the IT world's highlights to develop better goods and services.

In a different approach, it is also interesting to note the Ukrainian diaspora. According to projections from the 2019 census, there are over 1 million Americans with Ukrainian ancestry[203]. According to data from the American Community Survey from 2016 to 2020, California has one of the largest Ukrainian communities in the USA, with about 60,000 immigrants hailing from the country (second only to New York with 75,000). California is home to almost one in six Ukrainian immigrants living there[204]. Ukraine has long been one of Silicon Valley's go-to offshore hubs for skilled, affordable IT workers. The Ukrainian consulate in San Francisco estimates that there are currently 20,000 persons of Ukrainian descent living in the Bay Area. The ties between the two areas go beyond just commerce, where strong affinities between cultures have grown. People collaborate on projects while traveling between the Bay Area and Ukraine, and many exchange vows of marriage[205]. With this information, it is possible to foresee the significant relationship between the USA and Ukraine, with a great feeling of empathy and compassion. Connected to this, it is possible to address that since the Maidan Plaza events in 2014, Ukraine's tech sector, primarily comprised of IT consulting companies and software developers, has been expanding at double-digit yearly rates. As a result, a new class of young, wealthy workers has emerged with strong ties to the West thanks to their clients in the USA and EU[206].

The Hybrid Threat Environment is the last issue to consider in this context. Hybrid threats are a collection of several tools used to accomplish an unstated strategic goal without formally admitting it. In accordance with "The landscape of

---

[202] https://www.analyticsinsight.net/google-amazon-microsoft-who-is-leading-the-ai-race/
[203] https://data.census.gov/table?q=b04006&t=Ancestry&tid=ACSDT1Y2019.B04006
[204] Ukrainian Immigrants in California - Public Policy Institute of California (ppic.org)
[205] https://www.kqed.org/news/11906302/why-russias-invasion-of-ukraine-is-personal-for-silicon-valley
[206] https://www.forbes.com/sites/amyfeldman/2022/04/04/for-ukraines-tech-startups-fighting-the-war-means-memes-information-campaignsand-keeping-their-businesses-going/

hybrid threats: A conceptual model"[207], issued in 2021 by the European Commission and the Hybrid CoE39, the annexation of Crimea in 2014 marked the beginning of the political use of the terms Hybrid Threats and Hybrid Warfare. And the "*Political use of Hybrid Threats refers to manipulative, unwanted interference through a variety of tools: spread of disinformation/misinformation, creation of strong (but incorrect or only partially correct) historical narratives, election interference, cyber-attacks, economic leverage, to name just a few. Some of the activities may not even be illegal per se*."

A few days before the invasion of Ukraine by the Russian Federation, on 24 February 2022, the term HYBRID appeared in several magazines and newspapers. For example, in the Economist[208], on 22 February 2022, an article with the title "What is hybrid war and is Russia waging it in Ukraine" highlights "An old idea acquires new dimensions in a globalised world", noting that the fighting along the "line of control" between Ukrainian forces and separatists is considered "hybrid war". Another example, by Deutsche Welle (DW), on 18 February 2022, an article written by Frank Hofmann[209], a reference in this subject, with the title "Russia's hybrid war against Ukraine" stating that "Mercenaries, cyber-attacks, targeted disinformation - Russia no longer depends on classical methods of warfare in its campaign to destabilize Ukraine", and mentions the reasons why the Kremlin was pushing hard to escalate the hybrid war. The Security Magazine[210] published on 17 February 2022 the "Global hybrid warfare introduces cyber threats to companies amid the Russia-Ukraine crisis" stating, "The landscape of conflict today does not only feature active physical combatants — but instead also places companies in sectors such as energy, supply, healthcare, transportation and banking in digital crosshairs." This term has become more familiar in the media environment. The 2018 article, "The Russian hybrid war of the "little green men" and the impact on NATO", written by Manuel Mota43 in the EuroDefense Portugal magazine encapsulates the new approach to warfare which started 10 years ago and concludes by saying "Russia won the "military war" and the "information war" to support its combat operations in Crimea and undermine Western enthusiasm for eventual direct involvement.

---

[207] https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/
[208] https://www.economist.com/the-economist-explains/2022/02/22/what-is-hybrid-war-and-is-russia-waging-it-in-ukraine
[209] https://www.dw.com/en/russias-hybrid-war-against-ukraine/a-60829873
[210] https://www.securitymagazine.com/articles/97103-global-hybrid-warfare-introduces-cyber-threats-to-companies-amid-the-russia-ukraine-crisis

However, the essence of "hybrid war" requires synchronising, sequencing and combining the several instruments of State Power in order to win the underlying "political war", an effort without which one cannot achieve the desired end state."

Following the invasion of Ukraine in February 2022, Russia's cyberattacks on that country have accelerated dramatically, threatening the Ukrainian internet and endangering vital data, services, and infrastructure in an effort to undercut Ukraine's sovereignty and military edge.

The research for this document was conducted with western and Ukrainian sources from October 2022 to January 2023, which can provide a non-global view of all the facts needed for an independent analysis.

2. INSTITUTIONAL SUPPORT TO UKRAINE – COUNTRIES, ORGANIZATIONS AND COMPANIES

The international support for Ukraine in cyberspace has been increasingly significant since the invasion of Crimea in 2014. This event taken by the Russian Federation was considered a milestone in the political view of the Russian action, as mentioned before, and is the reason for the different approach by western countries/ International organizations (NATO/EU).

Almost a year after the invasion, some cyberspace reports were issued. Note the "Russia's war on Ukraine: Timeline of cyber-attacks" from the European Parliament[211], showing the public, energy, media, financial, commercial, and non-profit sectors in Ukraine who suffered the most from 2014 until February 2022. After this date, phishing emails, distributed denial-of-service attacks, data-wiper malware, backdoors, surveillance software, and information thieves are some examples of other dangerous online behaviour. The hybrid risks presented have not gone unnoticed by organizations and governments worldwide, with an impact on the supply of food, medicine, and humanitarian aid.

Also consider the Carnegie Endowment for International Peace report, by Nick Beecroft, on the "Evaluating the International Support to Ukrainian Cyber Defence"[212]. It states that a significant rise in capabilities and capacity has been achieved due to the worldwide effort to support Ukrainian cyber defence, which

[211] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549
[212] https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322

has brought together a wide range of players to conduct operations at a constant high pace. One of the many arguments put forward, to explain the comparatively minor influence of cyber operations in the war, has been the international effort in cyberspace to strengthen Ukraine in several dimensions. And concludes by stating "the integration of commercial actors as agents of foreign and defence policies and the reality that a handful of American companies are indispensable to large-scale cyber defence" expressing a real view of the international support provided to Ukraine.

The Science and Technological Committee of the NATO Parliamentary Assembly46 issued a report at the end of 2022[213], about Technological Innovation forFuture Warfare and provided some earliest observations of the Ukraine war and the implications it may have for future warfare. It analyzed four technological areas: satellites, drones, mobile phone cameras, and cyberspace. The last three points were emphasized: (1) before the war, the western support to Ukraine to strengthen its cyber defences, particularly from the United States; (2) the support received by Ukraine from private companies, which have shielded networks and critical infrastructure and (3) the "IT army" established by Ukraine.

To understand how deeply the two initial points are, the methodology adopted in this study considers Cyberspace as the object of study, and a qualitative research strategy was adopted based on a literature review (100%). The delimitations are: (1) Context - the International Support to Ukraine in cyberspace; (2) Temporal - period 2014-Jan2022; (3) Geographic - Ukraine; (4) Sources of Information - the information available in the Western Countries and Ukraine. Note that cyberspace has been intensely used for information and psychological warfare, but this analysis does not consider these dimensions...

2.1. Support provided to Ukraine before the invasion on 24th February 2022

2.1.1. United States of America (USA)

The relationship between the USA and Ukraine in Cyberspace has several scopes[214].

---

[213] https://www.nato-pa.int/download-file?filename=/sites/default/files/2022-11/025%20STCTTS%2022%20E%20rev.1%20fin%20-%20THE%20FUTURE%20OF%20WARFARE%20-%20FRIDBERTSSON%20REPORT.pdf

[214] https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/

Law enforcement – The Federal Bureau of Investigation (FBI) has given its Ukrainian partners direct support, briefing them on Russian intelligence services' cyber operations, exchanging cyber threat information about potential or ongoing malicious cyber activity, assisting in the disruption of nation-state efforts to disseminate disinformation and target the Ukrainian government and military, and exchanging investigative techniques on cyber incidents.

Technical – The US Agency for International Development (USAID) has supported the Ukrainian government's critical infrastructure operators and government ministries with technical experts to identify malware and restore systems after an incident has occurred. The ambitious $38 million USAID cybersecurity reform program of 2020 to improve Ukraine's cybersecurity legal and regulatory environment and connect critical infrastructure operators and private sector solution providers was developed to increase Ukraine's cyber workforce. The US Agency for International Development (USAID) has given the Government of Ukraine 5,000 Starlink Terminals through a public-private partnership with the American aerospace manufacturer SpaceX[215].

Financial – Since 2017, the US Department of State has given Ukraine $40 million in cyber development assistance. In 2020, as part of a "cyber dialogue" between the two nations, the State Department announced a new support to Ukraine with $8 million in cybersecurity assistance[216].

“Hands on” - Between December 2021 and March 2022, the US CYBER COMMAND joint forces worked closely with the Ukrainian government to conduct defensive cyber operations with Ukrainian Cyber Command personnel as part of a larger initiative to improve the cyber resiliency in national critical networks. Within two weeks, their mission - which included about 40 troops from the US armed services - became one of its largest deployments[217]. The most extensive search forward squad was sent out by US Cyber Command, with US Navy and US Marine Corps personnel working together to search for harmful online activity on Ukrainian networks. The operation continued until a few days before Russian soldiers began a massive invasion of the country[218].

---

[215] https://www.usaid.gov/news-information/press-releases/apr-05-2022-usaid-safeguards-internet-access-ukraine-through-public-private-partnership-spacex
[216] https://www.trade.gov/market-intelligence/ukraine-cybersecurity-assistance
[217] https://www.bbc.com/news/uk-63328398
[218] https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/

2.1.2. NATO – The cyber support to Ukraine can be seen in two dimensions:

Capability Development - Through the NATO-Ukraine Cyber Defence Trust Fund[219], in 2015, laboratories were created to look into cyber security occurrences as well as the creation of an incident management centre to monitor cyber security events. Additionally, the project offers instruction to staff on how to use these tools and technologies and helpful guidance on formulating policies. This project was led by Romania and had a value of 965,000 €[220].

Technology – through the access of Ukraine to NATO's Malware Information Sharing Platform (MISP)[221] to enable information sharing on the technical aspects of malware within the Allied community.

2.1.3. EU – Two dimensions can be considered:

Capability Development – In December 2020, the European Union started a €25 million project to aid Ukraine in its digital transformation and integration with the EU Digital Single Market. The most significant bilateral EU e-governance and digital program in any partner nation is called EU4DigitalUA56. Since 2012, complex e-government projects have been successfully carried out in Ukraine by the Estonian E-Governance Academy[222].

Technical support – On 22 February, following a request from Ukraine to help the country's institutions facing cybersecurity challenges, the Cyber Rapid Response Teams (CRRTs) were activated[223]. The CRRTs is a project developed within the EU's Permanent Structured Cooperation (PESCO) framework to respond to cyber incidents. Led by Lithuania with other five EU Member States, it will enable the member nations to cooperate to ensure greater levels of cyber resilience and respond to cyber incidents as a group[224]. The CRRTs project has been operational since 2019 and, in May 2021, became the first of the 60 PESCO projects to acquire

---

[219] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_02/20150203_1502-Factsheet_PracticalSupport.pdf
[220] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160712_1606-trust-fund-ukr-cyberdef.pdf
[221] https://www.nato.int/cps/en/natohq/news_190850.htm
[222] https://eufordigital.eu/new-eu4digitalua-project-supports-digital-transformation-in-ukraine/
[223] https://twitter.com/lithuanian_mod/status/1496078679960702978
[224] https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

Full Operational Capability (FOC)[225]. To highlight that for the first time, a capability developed within the framework of EU's PESCO project has been formally activated in an operational context, and it consists of 8-12 cybersecurity experts pooled from six countries of the project.

2.2. Support provided to Ukraine after the invasion

2.2.1. IT Private Companies

Cyberattacks targeting Ukrainian companies, websites, and government institutions were part of the full-scale military invasion of Ukraine on February 24. Since then, Kiev has also been supported by the private sector on cybersecurity[226], and "Operational cyber defence assistance provided by private companies has proven highly effective for Ukraine in helping sustain the ability to operate in the digital space"[227]. Many organisations in the cybersecurity industry, where several start-ups are considered, have started to take action to help and support those directly and indirectly touched by cyber incidents connected to the Ukraine-Russia war[228]. Amongst them, there are Artificial Intelligence companies, like Vectra AI[229]- which offers several services on a complimentary basis, which include scanning of Microsoft Azure Active Directory (AD), Microsoft 365 and AWS environments for signs of attack and surveillance of network infrastructure; Avast[230] - a Cybersecurity software company that researches and develops computer security software, machine learning and artificial intelligence; Endpoint Protection Platforms like CrowdStrike[231] - an international leader or Global Network Company like Cloudflare[232] - designed to make the Internet more secure, private, fast, and reliable; and software-defined networking companies like CISCO[233] - delivers innovative software-defined networking, cloud, and security solutions. Although

[225] https://eda.europa.eu/news-and-events/news/2022/02/24/-of-first-capability-developed-under-pesco-points-to-strength-of-cooperation-in-cyber-defence#
[226] https://www.cfr.org/blog/ukrainian-cyber-war-confirms-lesson-cyber-power-requires-soft-power
[227] https://www.crdfglobal.org/news/crdf-global-becomes-platform-for-cyber-defense-assistance-collaborative-cdac-for-ukraine-receives-grant-from-craig-newmark-philanthropies/
[228] https://www.foreignaffairs.com/ukraine/big-tech-goes-war
[229] https://www.vectra.ai/news/as-the-war-in-ukraine-spirals-vectra-ai-announces-free-cybersecurity-services
[230] https://blog.avast.com/avast-response-to-war-in-ukraine
[231] https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-against-wiper-malware-used-in-ukraine-attacks/
[232] https://blog.cloudflare.com/tag/ukraine/
[233] https://www.cisco.com/c/m/en_us/crisissupport.html

the companies mentioned above, amongst many others, have decided to support Ukraine, there are three that need to be deeply addressed: Amazon, Microsoft, and Google, due to the value they have in the technological global market and the support to Ukraine. We are talking about three of the five Big Techs.

2.2.2. Amazon Web Services (AWS)

Generically, AWS helps organizations design a cybersecurity analytics platform that unifies data, analytics, and Machine Learning (ML)[234], which includes four capabilities: Behavioral analytics, Security investigation, Predictive security analytics, and Automated monitoring. The leadership company on cloud services[235], assisted in safeguarding crucial data to ensure the continued operation of Ukraine's banking, educational, and government sectors[236]. Ukrainian law mandated that certain government data and specific private sector data be kept on servers physically situated in Ukraine before the Russian invasion. One week before the Russian military invasion, the Ukrainian parliament authorized laws allowing the transfer of public and private sector data to the cloud. Then, the Ukrainian government issued a public plea for assistance to achieve that, and AWS was one of the first firms to respond. Its members met with Ukrainian government officials on February 24, the invasion day, to assist in securing, storing, and moving data to the cloud. Despite all the physical damage, the government can still look after its citizens. That hasn't typically been the case in wars or severe weather events where people and governments are frequently compelled to start rebuilding nearly from scratch. In light of this, it is understandable why data has evolved into a target in modern warfare and a crucial asset to safeguard. The information transferred to the cloud represents the lives and the country that Ukrainians want to regain and reconstruct after the war. Since the start of the conflict in Ukraine, Amazon has given more than $45 million in resources, goods, and cloud computing credits to charities operating locally to support Ukrainian citizens and institutions[237]. AWS has pledged $15 million in cloud computing credits and technical help. In addition

---

[234] https://aws.amazon.com/blogs/publicsector/how-create-cybersecurity-analytics-platform-aws-analytics-machine-learning/
[235] https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/
[236] https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future
[237] https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine

to powering applications that facilitate the intake of Ukrainian refugees at border crossings, AWS technologies and experts have been assisting in various activities, including setting up emergency internet connectivity, establishing safe evacuation routes, and enabling secure communications[238]. AWS provided USD 75 million[239] to support Ukraine in migrating state registers and other vital state databases to the AWS cloud environment as well as the ITSkills4U programme75.

2.2.3. Microsoft

Microsoft has introduced numerous AI solutions in a variety of industries[240]. By learning from the data of every business that uses its services, Microsoft employs AI to combat cybercriminals and the business' Azure security team creates protection specific to a client's online activity.

Regarding this conflict, Microsoft announced it was significantly reducing its business in Russia, joining several firms that have done so in response to the invasion by reducing their exposure or leaving the country[241]. During the last Web Summit in Lisbon in November 2022, Microsoft announced it would give Ukraine additional support of approximately $100 million in technical assistance, boosting its overall funding for Ukraine to more than $400 million since the crisis began in February. Through 2023, it will continue to provide Ukraine with free technology support as Russia's invasion of the nation continues[242]. In a blog post, Microsoft Corp President Brad Smith wrote that it "will ensure that government agencies, critical infrastructure, and other sectors in Ukraine can continue to run their digital infrastructure and serve citizens through the Microsoft Cloud"[243]. To highlight are the regular Microsoft Special Reports on Ukraine, providing insights into the scope, scale, and methods of Russia's use of cyber capabilities as part of the large-scale "hybrid" war in Ukraine and offering strategic recommendations to organizations worldwide. In 2022, three reports with strategic and technical detailed information were issued.

---

238 https://www.aboutamazon.com/news/community/amazon-continues-donating-to-help-ukrainian-refugees

239 https://www.kmu.gov.ua/en/news/amazon-web-services-nadaye-ukrayini-pidtrimki-na-75-mln-dolariv-na-hmarni-tehnologiyi-yaki-dopomagayut-stabilno-pracyuvati-cifrovij-derzhavi-ta-ekonomici

240 https://www.analyticsinsight.net/google-amazon-microsoft-who-is-leading-the-ai-race/

241 https://www.reuters.com/technology/microsoft-cuts-russia-operations-due-ukraine-invasion-bloomberg-2022-06-08/

242 https://www.reuters.com/technology/microsoft-extends-free-tech-support-ukraine-through-2023-2022-11-03/

243 https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/

In the first report, "An overview of Russia's cyberattack activity in Ukraine"[244], issued in April, Microsoft assessed that the climate of urgency might encourage the employment of sensitive tools that give threat actors secure access to networks or the ability to tamper with specific components of information systems in order to further their strategic goals. In the medium term, highly restricted capabilities like zero-days, attacks on crucial infrastructure, supply-chain attacks, and other cutting-edge methods would almost surely be on display. The linkage between the Cyber intrusions before the kinetic actions in several events was also proved.

In the second report, "Defending Ukraine: Early Lessons from the Cyber War"[245], issued in June, it was stated that "The Russian military poured across the Ukrainian border on February 24, 2022, with a combination of troops, tanks, aircraft, and cruise missiles. But the first shots were, in fact, fired hours before when the calendar still said February 23. They involved a cyberweapon called "Foxblade" that was launched against computers in Ukraine". It was also mentioned that the cyber components of the ongoing conflict go well beyond Ukraine and highlight the distinctive characteristics of cyberspace.

The last 2022 report, "Preparing for a Russian cyber offensive against Ukraine this winter"[246], issued in December, noted that Moscow has stepped up its hybrid technology campaign to pressure the domestic and international sources of Kiev's military and political support. So, missile strikes knocked out power and water supply to civilians nationwide, and cyberthreat actors connected to Russian military intelligence launched destructive wiper attacks against energy, water, and other critical infrastructure organizations' networks in Ukraine. In an apparent effort to obstruct the flow of supplies and weaponry to the front, Russian military operators also increased their harmful cyberactivity to Poland, a crucial logistics hub.

2.2.4. Google

As part of its DDoS protection and web application firewall (WAF) service[247], Google offers customers the same technology it employs to protect itself: Cloud Armor Adaptive Protection84. In order to identify potential threats, this system

[244] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
[245] https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
[246] https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/
[247] https://www.zdnet.com/article/google-is-using-machine-learning-to-stop-ddos-attacks/

analyses signals from various web services using machine learning (ML) models. By recognizing unusual traffic, it may quickly mitigate huge volume application-layer DDoS assaults against web apps and services.

The most used website worldwide and the most popular search engine in the West are both called Google[248], which announced the increase in security measures to help protect Ukrainian civilians and websites after the invasion. Kent Walker, the company's President of Global Affairs[249], made the declaration with several steps, which include SOS alerts on its Search function, automated detection and blocking of suspicious activity, Gmail notifications of government-backed attack warnings, increased authentication challenges, and the expansion of its Advanced Protection and Project Shield programs. Also, the Threat Analysis Group (TAG)[250], is a group that aims to defend consumers against sophisticated, persistent threats and state-sponsored malware attacks. TAG keeps a close eye on threat actors and how their strategies change, actively monitoring and thwarting campaigns directed at Ukrainian citizens and organizations releasing information on Russian threat actors[251].

Mandiant, acquired by Google in March 2022, is a leader in dynamic cyber defence and incident response services[252], has been delivering unparalleled frontline expertise and industry-leading threat intelligence for the past 18 years[253]. With this market decision, Google can, therefore, provide better cybersecurity services to its customers and, consequently, to Ukraine.

2.3. Satellite Services – Starlink

The private spaceflight business SpaceX created the satellite network known as Starlink to bring inexpensive internet to isolated areas. This is the first and largest satellite constellation in the world[254]. It uses a low Earth orbit to provide broadband internet that can enable streaming, online gaming, video calls, and other activities. Starlink provides customers with high-speed, low-latency internet around the globe by utilizing cutting-edge satellites in a mega constellation of

[248] https://techmonitor.ai/what-is/what-is-google
[249] https://therecord.media/google-expands-security-protections-for-ukrainian-users
[250] https://blog.google/threat-analysis-group/googles-efforts-to-identify-and-counter-spyware/
[251] https://blog.google/threat-analysis-group/
[252] https://cloud.google.com/blog/products/identity-security/google-completes-acquisition-of-mandiant
[253] https://www.mandiant.com/company/press-releases/google-acquire-mandiant
[254] https://www.starlink.com/technology

42,000 satellites when the Full Operational Capability is achieved[255]. By now, there are about 3,000 satellites around the Earth.

After the invasion, by 26 February, Mykhailo Fedorov, the Ukrainian minister of digital transformation, requested on Twitter[256] the support of Starlink. Elon Musk, the creator of SpaceX, decided to give Starlink to Ukraine for free in response, by 28 February, and responded also in Twitter, "Starlink service is now operational in Ukraine"[257]. Despite power outages and Russian strikes on the nation's internet infrastructure, many Ukrainians, most notably the military, stayed online thanks to Musk's satellite communication system Starlink[258]. Even in the absence of alternative internet infrastructure or during power outages, Starlink enables access to the internet. Additionally, experts claim that it is nearly impossible for Russian troops to intercept, making it more secure than other forms of communication. It is simple to use, as installing a Starlink dish and connecting to satellite internet only takes up to 20 minutes. More than25,000 Starlink terminals have been delivered to Ukraine[259] from foreign partners, volunteers, or directly from SpaceX, which shows a tremendous logistic company's ability, and the Ukrainian soldiers can use drones anywhere and relay data fast to a command centre that analyses the footage and organizes strikes against the Russian military troops.

By using this satellite network for both military and civilian purposes, Ukraine has foiled Russia's attempts to cut off the Eastern European nation from the outside world, providing Kiev with a much-needed victory over Moscow in a conflict that shows no signs of coming to an end[260]. In accordance with BGEN Steve Butow, director of the space portfolio at the Defence Innovation Unit, the Pentagon's Silicon Valley tech outpost, said, "The strategic impact is, it totally destroyed Vladimir Putin's information campaign. He never, to this day, has been able to silence Zelensky."[261]

Elon Musk's Starlink is helping Ukraine to win the drone war as the Ukrainian military is using Starlink satellite system to locate and kill invading

---

[255] https://www.space.com/spacex-starlink-satellites.html
[256] https://twitter.com/FedorovMykhailo/status/1497543633293266944
[257] https://kyivindependent.com/how-elon-musks-starlink-satellite-internet-keeps-ukraine-online/
[258] https://kyivindependent.com/how-elon-musks-starlink-satellite-internet-keeps-ukraine-online/
[259] https://www.space.com/ukraine-spacex-starlink-terminals-offline-funding-shortfall
[260] https://www.politico.eu/article/elon-musk-ukraine-starlink/
[261] https://www.news18.com/news/world/starlink-has-destroyed-vladimir-putins-information-campaign-says-us-official-5348929.html

forces[262]. A unit named Aerorozvidka (Aerial Reconnaissance) is at the forefront of Ukraine's astoundingly successful military campaign against Russian soldiers. This outfit uses attack and surveillance drones to hit Russian tanks and positions. The advanced "Delta" technology, developed in recent years with assistance from foreign allies[263], is used by the Ukrainian drone unit and is accessible from inexpensive PCs. It has "situational awareness" software that builds an interactive map using data from sensors, drones, satellites, and human intelligence to locate the opponent. According to reports, Delta has been tested at the Sea Breeze military exercise in the Black Sea, which included the USA, Ukraine, and 30 other countries, and is interoperable with NATO systems. The Ukrainian system benefited from Western nations' equipment donations, such as radio communications that were more advanced than Soviet-era technology. The USA has also invested millions of dollars to defend against Russian hacking, signal jamming, and attempts to "spoof" GPS technology[264].

The Pentagon believes that providing Ukraine with planes is no longer essential because drones are proven to be so effective. Instead, it has been deploying more potent Switchblades, known as "kamikaze drones," which are small enough to fit in a backpack and are capable of destroying tanks, which were created for USA special forces[265].

As other internet services were unavailable due to war damage, power outages, jamming, or simply because the locations were remote, the country's military quickly came to rely on Musk's network[266]. Without early and cheap access to Starlink satellite internet technology, Ukrainian networks could not have survived[267].

---

[262] https://www.telegraph.co.uk/world-news/2022/03/18/elon-musks-starlink-helping-ukraine-win-drone-war/
[263] https://mil.in.ua/en/news/ukraine-unveiled-its-own-delta-situational-awareness-system/
[264] https://www.telegraph.co.uk/world-news/2022/03/18/elon-musks-starlink-helping-ukraine-win-drone-war/
[265] https://fedscoop.com/american-kamikazes-pentagon-has-big-plans-for-suicide-drones/
[266] https://www.theguardian.com/world/2023/feb/09/zelenskiy-aide-takes-aim-at-curbs-on-ukraine-use-of-starlink-to-pilot-drones-elon-musk
[267] https://www.cfr.org/blog/ukrainian-cyber-war-confirms-lesson-cyber-power-requires-soft-power

2.4. International Organizations

2.4.1. NATO

Ukraine was accepted as a Contributing Participant to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in 2022. This multinational Centre of Excellence was founded in 2008 in Tallinn, Estonia, and accredited by NATO. The mission is to support "member nations and NATO with unique interdisciplinary expertise in cyber defence research, training and exercises covering the focus areas of technology, strategy, operations, and law"[268].

Regarding cyber intelligence operations against Russia, there have been rumours that NATO forces have given targeting information for valuable targets such as command centres and ammunition stockpiles[269].

2.4.2. EU

By October 2022, the EU invested more than €10 million to improve cybersecurity and maintain access to public services in Ukraine[270]. By February 2023, the "EU Support to Strengthen Cyber Security in Ukraine" project is promptly responding to the nation's data security and cybersecurity demands.

2.5. Countries

2.5.1. United States of America

The USA reinforced the support with another $45 million added in 2022 to help Ukraine improve its cyber defensive capabilities[271]. The US Cybersecurity and Infrastructure Security Agency (CISA) released a warning updated by 28 April 2022[272] with technical information and advice for preventing the use of dangerous malware targeting Ukrainian enterprises. In July 2022, this agency signed a Memorandum of Cooperation (MOC) with the Ukrainian State Service of Special Communications and Information Protection of Ukraine (SSSCIP) to

[268] https://ccdcoe.org/about-us/
[269] https://www.bakerinstitute.org/research/cyber-and-information-warfare-ukraine-what-do-we-know-seven-months
[270] https://eufordigital.eu/eu-supports-cybersecurity-in-ukraine-with-over-e10-million/
[271] https://it.usembassy.gov/protecting-ukraines-internet-access-and-critical-data/
[272] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a

strengthen collaboration on shared cybersecurity priorities[273]. The USA has also been very active through the Cyber National Mission Force disclosing Indicators Of Compromise (IOCs) from Ukrainian networks. The IOCs serve as digital forensics for network defenders in the event of a potential breach and serve as proof of potential intrusions on a host machine or network. Users can search for and find malware on the host machine or network thanks to the installation of IOCs[274]. General Paul Nakasone first acknowledged that the USA had "conducted a series of operations" in reaction to Russia's invasion of Ukraine in an exclusive interview with Sky News[275]. He confirmed to Sky News: "*We've conducted a series of operations across the full spectrum; offensive, defensive, [and] information operations*." The revelation highlights how crucial it has been for the USA to project cyberspace power to support Ukraine's defences and possibly deter Russia from launching cyberattacks against USA infrastructure.

2.5.2. United Kingdom

In response to an uptick in Russian cyber activities in the days after the invasion of Ukraine, a £6.35 million package was mobilized[276]. Protecting the Ukrainian government and its vital national infrastructure from harmful cyberattacks is the goal of the UK's Ukraine Cyber Programme. By working together with industry, the aim is to keep malicious actors off key networks and provide Ukrainian authorities access to forensic tools. The National Cyber Security Centre NCSC has been assisting Ukraine's online security forces).

3. HACKTIVISM - IT ARMY

With the Russian invasion, Ukraine faced challenging times, naturally. A Tweet posted by Mykhailo Fedorov, the vice prime minister and minister of Ukraine's digital transformation, on February 26, attracted worldwide attention, notifying that Ukraine was forming a volunteer IT army to fight Russia online. This

---

[273] https://www.cisa.gov/news-events/news/united-states-and-ukraine-expand-cooperation-cybersecurity

[274] https://www.cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks/

[275] https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139

[276] https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defences-with-6-million-support-package

tweet was linked to a Telegram channel where a list of well-known Russian websites was released[277]. He also stated, "There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists". Ukraine uses cyber tools to harass Russia, namely targeting the railways, the energy grid, and the websites of governmental and financial institutions as the main objectives[278]. In a post translated into English, the channel said, "We encourage you to use any vectors of cyber and DDoS attacks on these resources"[279], referring to distributed denial of service attacks that flood websites with malicious traffic to knock them offline.

Many volunteers with IT and internet experience from the Ukrainian population and outside this country adhered to the "IT Army of Ukraine" to conduct a "digital war" against Russia. This was made possible by the fact that Ukraine has a comparatively developed cybersecurity industry, a sizable pool of qualified engineers, and a significant diaspora linked with the IT industry.

Although Ukraine has enlisted thousands of cybersecurity professionals in the war through the IT Army, no one knows precisely who they are and how many they are. The number of "IT Soldiers" was/will never be well known. To show excellent adherence, some examples were provided, where tapping 'Join' on the public channel is all it takes and considering the first week of the war: by 27th February, about 175,000 people have subscribed[280], or 240,000[281]; and by 2nd March 250,000[282] or even to 275,000[283]. But one month later, by 7th April, the Royal United Services Institute (RUSI), the world's oldest and the UK's leading defence and security think tank, presented another number of 175,000[284].

The IT Army volunteers have different motives, different types of expertise, and other abilities to use cyber weapons[285]. There are also Script kiddies' volunteers

---

277 https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/

278 https://www.nato-pa.int/download-file?filename=/sites/default/files/2022-11/025%20STCTTS%2022%20E%20rev.1%20fin%20-%20THE%20FUTURE%20OF%20WARFARE%20-%20FRIDBERTSSON%20REPORT.pdf

279 https://www.nytimes.com/live/2022/02/27/world/russia-ukraine-war#ukraine-russian-websites

280 https://blog.checkpoint.com/security/how-the-eastern-europe-conflict-polarized-cyberspace/

281 https://www.theaustralian.com.au/world/hacktivists-wage-cyber-offensive-on-websites/news-story/3cf1ab971b719356722765aa3b28aaf7

282 https://www.abc.net.au/news/2022-03-02/hackers-answer-call-in-ukraine-russia-war/100873490

283 https://ncfacanada.org/ways-you-can-help-support-ukraine/

284 https://rusi.org/explore-our-research/publications/commentary/tweet-mightier-sword-debunking-disinformation-ukraine

285 https://www.dw.com/en/ukraines-it-army-who-are-the-cyber-guerrillas-hacking-russia/a-61247527

with little experience in cybersecurity who run hacker programs without fully understanding how they work. Anonymous123 is also a powerful player in Ukraine's cyber guerrilla army. By February 27, Anonymous claimed hacks on more than 300 Russian cyber targets in 48 hours, including the Gas Control System. Hackers also claimed to have broken into the Tetraedr military company in Belarus, stealing over 200 terabytes of emails and then exposing the data[286].

Tim Stevens, a senior lecturer in global security at King's College London, concerned with this phenomenon, warned that there are many unexplored and hypothetical scenarios when it comes to cyberattacks and highlighted the possibility of escalation. "What concerns me is if there are non-Ukrainians and Russians involved in this because that is effectively an internationalization of the cyber aspect of this conflict and could be treated by either combatant as a de facto escalation of the conflict beyond Ukraine's borders."[287]

Another apprehension is with cybercrime. According to a survey by Accenture[288], the world of cyber criminals is currently divided between supporters of Russia and Ukraine. Accenture's Cyber Threat Intelligence team tracks illicit activities on the dark web and noted in its research that, for the first time, financially driven hackers are divided into ideological factions.

Many Western responsible actors[289], such as Rob Joyce, the NSA's Director of Cybersecurity, and Lindy Cameron, the head of the UK's National Cyber Security Centre (NCSC), alleged that Western nations are concerned about the resurgence of hacktivists. Ukraine hacktivism is potentially dangerous as it exposes oneself, which could have personal repercussions. "When Anonymous was active it encouraged supporters to download and use the Low Orbit Ion Canon (LOIC)128 to launch DDoS attacks against websites. Many of the participants in this activity were easily identified and subsequently charged with cybercrime activities." as Javvad Malik, lead security awareness advocate at security training platform Knowbe4, stated[290].

To note also is the position of Jason Healey, a senior research scholar at Columbia University's School for International and Public Affairs, part-time

---

[286] https://www.hstoday.us/subject-matter-areas/cybersecurity/anonymous-claims-hits-on-more-than-300-russian-cyber-targets-in-48-hours-including-gas-control-system/
[287] https://www.wired.co.uk/article/ukraine-it-army-russia-war-cyberattacks-ddos
[288] https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog-14MARCH22.pdf
[289] https://techmonitor.ai/technology/cybersecurity/ukraine-hacktivism-problematic-nsa-ncsc
[290] https://techmonitor.ai/technology/cybersecurity/ukraine-hacktivism-problematic-nsa-ncsc

strategist at the Cybersecurity and Infrastructure Security Agency (CISA) and who has held cyber positions at the White House, Goldman Sachs, and the US Air Force, stating that "While government support for patriotic hacking is not unprecedented, the Ukrainian campaign stands in stark violation of recently agreed-to norms on state behaviour in cyberspace, as well as the foreign policy positions of NATO members and the European Union"[291].

4. ANALYSIS

To understand the international support to Ukraine in cyberspace, it was possible to realize that the scale and influence of the cyber dimension in today's political and military conflicts are difficult to foresee. Whether there is peace or conflict, leaders/decision-makers, societal systems, and the public can all be targets. Therefore, the digital dimension is part of the traditional national security risks portfolio. The reality of cyberspace in the Russia-Ukraine conflict proves what Joseph Nye, in his book "Cyber Power", alludes to the diffusion of power, where States have to share the stage with non-state actors, demonstrating that they have a growing power. And this is not only in the technological arena but also in the relevance of geopolitical power, with the reinforcement of one of the conflicting parties.

Thus, in cyberspace and in the context of this article, the international institutional support to Ukraine has been substantial and can be divided into three main types:

By the USA, directly and indirectly. Directly through government agencies and departments, as well as the US Cybercommand, with extensive financial and technical support to build Ukraine's pre-invasion and post-invasion cyber capabilities since from February 2022, supplemented with support in the field of military operations, through experts remotely and on the ground, as well as a new approach to information sharing, in the interest of defeating Russia, as stated by John J. Mearsheimer[292]. Indirectly, together with the EU, imposed economic sanctions on Russia, including the withdrawal of Western companies from Russian territory, which were accompanied by specialists who left their country, and the privileged relationship with the Ukrainian diaspora in Silicon Valley.

By private companies, directly, considering two types:

---

[291] https://www.lawfareblog.com/patriotic-hacking-no-exception
[292] https://nationalinterest.org/feature/causes-and-consequences-ukraine-crisis-203182

Large technology companies, directly through high funding, monitoring, and acting proactively in cyberspace, allowing early warning to Ukrainian forces and their allies, as well as a contributory element to its continued use by Ukrainian society. AWS supported data migration to the cloud, which cannot be destroyed with missiles, where Microsoft's digital infrastructure has played a leading role for government agencies and in maintaining the functioning of critical infrastructures. The services provided by Google have helped to ensure safer use by Ukrainian society as well as to prevent attacks in cyberspace. These three Big Tech companies have artificial intelligence implemented in their products, providing situational awareness that incorporates predictive analytics. This automation of data analysis shortens the decision-making process and reduces the time needed to make decisions, giving the Ukrainians a leveraged edge over the Russians. Thus, the private sector has been a great ally, assisting Ukraine's resilience as it supports essential cybersecurity tools and intelligence, complementing its cybersecurity efforts, being the great guardians of cyberspace of Ukrainian interest.

Satellite service providers, like Elon Musk's Starlink network, making the internet available in the entire territory of Ukraine to support populations in accessing State services, as initially requested. Subsequently, there was a military use of the system for command and control purposes and for targeting Russian forces on the ground with great effectiveness. The use of Starlink is a novelty due to its speed and ease of service, being a state-of-the-art and low-cost technology with great versatility for users, whether civil or military. However, as this system is used for military purposes, it can always be considered a target, which can be a concern.

By the IT volunteers adhering to the IT Army, an initiative of the Ukraine government, where "everybody is inside" and the tasks to fight Russian infrastructure are issued in Telegram channels, a civil worldwide application. With the escalation of cyber operations, what will happen to all these fighters after the war? Western international experts are, naturally, concerned with what's happening in cyberspace, as the coherence between words and political decisions and acts is paramount.

Indeed, NATO and the EU, alongside other companies and countries, contributed to assisting Ukraine in cyberspace, albeit on a smaller scale compared to the aforementioned two entities. However, for interoperability, Ukraine's participation in the NATO CWIX exercise has contributed to greater knowledge and performance, as well as the financial support of the EU, embodying a considerable effort and explicit commitment.

Therefore, the new era of war demands greater international cooperation, where cyberspace security brings a new dimension to the conflict, and the existence of unique skills in this area is fundamental. The political construction of hybrid warfare is seen in this conflict, where cyberspace has a specific weight. However, the impact of cyberspace on achieving strategic outcomes was not as significant as anticipated, falling short of the expectations set by many experts in the field. Cyberspace constitutes an element with specific relevance, being fundamental for society and military operations. Not so much as a dominant element for operations in cyberspace, but as a support element for kinetic effects, where Starlink was a differentiating element by allowing access to the internet by the Ukrainian forces. The utilization of cyberspace has demonstrated an innovative approach, presenting us with a dilemma where both civilians and the military utilize systems in an undifferentiated manner, resulting in a widespread diffusion of its employment.

Additionally, it should also be noted that most companies that support Ukraine in cyberspace are American flag companies, even without a formal request from this administration, and many of which are acting pro bono. Assuming that these companies are not proxy-entities, this reality also presents challenges to the US executive insofar as, due to dimension of its action, it may affect the strategic objectives of the country in the international environment.

5. CONCLUSIONS

The international support to Ukraine in cyberspace has been a decisive point in this war. The commitment of countries, namely the USA and Great Britain, of private companies, some of the Big Techs and Starlink, and International Organizations constitutes an international coalition to defend Ukraine, although not formal, with significative results. The resurgence of hacktivism, now with characteristics associated to a State, is also a relevant aspect that this war brought to the international scene and is a concern.

Two significant ideas can be drawn from here: with the "Civilianization" and "Privatization" of the conflict between Russia and Ukraine, in a hybrid environment, the digital technology played a significant role in the current war, most of the time which is not visible. Furthermore, it might be shaping future geopolitics.

In this way, we can question whether another new stage of Revolution in Military Affairs is underway. This is because, according to Andrew Marshall, former Director of the Office of Net Assessments (Office of the Secretary of Defence),

a Revolution in Military Affairs (RMA) is a significant change in the nature of warfare brought about by the innovative application of new technologies [Starlink] which, combined with dramatic changes in military doctrine [Cyberspace] and operational [Drones] and organizational concepts [AI/ML], fundamentally alter the character [Private companies] and conduct [Big Tech companies] of military operations. According to what has been seen and what has been exposed in this document, we can infer that the established requirements to the RMA can be met.

AUTHOR's POSTFACE

Captain Helder Fialho de Jesus has a significant background and skills in cyber defence and in military operations. He previously served as the Head of the Portuguese Armed Forces Cyber Defence Centre between 2017 and 2020. In addition, he was the National Lead of the NATO CWIX exercise in 2018 and 2019 and represented Portugal in the Steering Committee of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), in Estonia. Prior to this role, he directed the Portuguese Navy Communications, Data and Cypher Centre (CCDCM) from 2015 to 2017. He also held a three-year NATO appointment at Supreme Headquarters Allied Powers Europe (SHAPE) – Belgium, where he focused on Communications and Information Systems in Joint Military Operations (J6). Presently, he is pursuing a PhD in International Relations-Strategy and Security Studies, at NOVA University of Lisbon – School of Social Sciences and Humanities (NOVA FCSH) Lisbon and collaborates with several entities in subjects such as Cyberspace and Hybrid Threats.

The main objective of the **Cadernos do IUM** is to disseminate the results of research developed at/under the aegis of the IUM, autonomously or in partnerships, not suitable to be published as a book.

Its publication should not have periodicity, however, at least six issues should be published annually. The themes should be in line with CIDIUM's priority lines of research. They should be published on paper and electronically on the IUM website.

The following are considered suitable to be published on Cadernos do IUM editorial line:

- Research work by CIDIUM researchers or other national or foreign researchers;
- Individual or group research work of recognized quality, carried out by students, in particular those of the CEMC and the auditors of the CPOG who have been nominated for publication and which fall within the scope of Military Sciences, National and International Security and Defense;
- Papers, essays and reflection articles produced by teaching staff;
- Communications by IUM researchers at scientific events (e.g., seminars, conferences, workshops, panels, round tables), whether national or international, in Portugal or abroad.

N.os Publicados:

1 – Comportamento Humano em Contexto Militar
Subsídio para um Referencial de Competências destinado ao Exercício da Liderança no Contexto das Forças Armadas Portuguesas: Utilização de um "Projeto STAfS" para a configuração do constructo
Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

2 – Entre a República e a Grande Guerra: Breves abordagens às instituições militares portuguesas
Coordenador: Major de Infantaria Carlos Afonso

3 – A Abertura da Rota do Ártico (*Northern Passage*). Implicações políticas, diplomáticas e comerciais
Coronel Tirocinado Eduardo Manuel Braga da Cruz Mendes Ferrão

4 – O Conflito da Síria: as Dinâmicas de Globalização, Diplomacia e Segurança
(Comunicações no Âmbito da Conferência Final do I Curso de Pós-Graduação em Globalização Diplomacia e Segurança)
Coordenadores: Tenente-coronel de Engenharia Rui Vieira
Professora Doutora Teresa Ferreira Rodrigues

5 – Os Novos Desafios de Segurança do Norte de África
Coronel Tirocinado Francisco Xavier Ferreira de Sousa

6 – Liderança Estratégica e Pensamento Estratégico
Capitão-de-mar-e-guerra Valentim José Pires Antunes Rodrigues

7 – Análise Geopolítica e Geoestratégica da Ucrânia
Coordenadores: Tenente-coronel de Engenharia Leonel Mendes Martins
Tenente-coronel Navegador António Luís Beja Eugénio

8 – Orientações Metodológicas para a elaboração de Trabalhos de Investigação
Coordenadores: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos
Tenente-coronel Técnico de Manutenção de Material Aéreo Joaquim Vale Lima

9 – A Campanha Militar Terrestre no Teatro de Operações de Angola. Estudo da Aplicação da Força por Funções de Combate
Coordenadores: Coronel Tirocinado José Luís de Sousa Dias Gonçalves
Tenente-coronel de Infantaria José Manuel Figueiredo Moreira

10 – O Fenómeno dos *"Green-on-Blue Attacks"*. *"Insider Threats"* – Das Causas à Contenção
Major de Artilharia Nelson José Mendes Rêgo

11 – Os Pensadores Militares
Coordenadores: Tenente-coronel de Engenharia Leonel José Mendes Martins
Major de Infantaria Carlos Filipe Lobão Dias Afonso

12 – *English for Specific Purposes* no Instituto Universitário Militar
Capitão-tenente ST Eling Estela do Carmo Fortunato Magalhães Parreira

13 – I Guerra Mundial: das trincheiras ao regresso
Coordenadores: Tenente-coronel de Engenharia Leonel José Mendes Martins
Major de Infantaria Fernando César de Oliveira Ribeiro

14 – Identificação e caraterização de infraestruturas críticas – uma metodologia
Major de Infantaria Hugo José Duarte Ferreira

15 – O DAESH. Dimensão globalização, diplomacia e segurança. Atas do seminário 24 de maio de 2016
Coordenadores: Tenente-coronel de Engenharia Adalberto José Centenico
Professora Doutora Teresa Ferreira Rodrigues

16 – Cultura, Comportamento Organizacional e *Sensemaking*
Coordenadores: Coronel Piloto Aviador João Paulo Nunes Vicente
Tenente-coronel Engenheira Aeronáutica Ana Rita Duarte Gomes S. Baltazar

17 – Gestão de Infraestruturas Aeronáuticas
Major Engenheira de Aeródromos Adelaide Catarina Gonçalves

18 – A Memória da Grande Guerra nas Forças Armadas
Major de Cavalaria Marco António Frontoura Cordeiro

19 – Classificação e Análise de Fatores Humanos em Acidentes e Incidentes na Força Aérea
Alferes Piloto-Aviador Ricardo Augusto Baptista Martins
Major Psicóloga Cristina Paula de Almeida Fachada
Capitão Engenheiro Aeronáutico Bruno António Serrasqueiro Serrano

20 – A Aviação Militar Portuguesa nos Céus da Grande Guerra: Realidade e Consequências
Coordenador: Coronel Técnico de Pessoal e Apoio Administrativo
Rui Alberto Gomes Bento Roque

21 – Saúde em Contexto Militar (Aeronáutico)
Coordenadoras: Tenente-coronel Médica Sofia de Jesus de Vidigal e Almada
Major Psicóloga Cristina Paula de Almeida Fachada

22 – *Storm Watching. A New Look at World War One*
Coronel de Infantaria Nuno Correia Neves

23 – Justiça Militar: A Rutura de 2004. Atas do Seminário de 03 de março de 2017
Coordenador: Tenente-coronel de Infantaria Pedro António Marques da Costa

24 – Estudo da Aplicação da Força por Funções de Combate - Moçambique 1964-1975
Coordenadores: Coronel Tirocinado de Infantaria Jorge Manuel Barreiro Saramago
Tenente-coronel de Infantaria Vítor Manuel Lourenço Ortigão Borges

25 – A República Popular da China no Mundo Global do Século XXI. Atas do Seminário de 09 de maio de 2017
Coordenadores: Professora Doutora Teresa Ferreira Rodrigues
Tenente-coronel de Infantaria Paraquedista Rui Jorge Roma Pais dos Santos

26 – O Processo de Planeamento de Operações na NATO: Dilemas e Desafios
Coordenador: Tenente-coronel de Artilharia Nelson José Mendes Rêgo

27 – Órgãos de Apoio Logístico de Marinhas da OTAN
Coordenador: Capitão-tenente de Administração Naval Duarte M. Henriques da Costa

28 – Gestão do Conhecimento em Contexto Militar: O Caso das Forças Armadas Portuguesas
Coordenador: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

29 – A Esquadra de Superficie da Marinha em 2038. Combate de alta Intensidade ou Operações de Segurança Marítima?
Capitão-de-mar-e-guerra Nuno José de Melo Canelas Sobral Domingues

30 – Centro de Treino Conjunto e de Simulação das Forças Armadas
Coronel Tirocinado de Transmissões Carlos Jorge de Oliveira Ribeiro

31 – Avaliação da Eficácia da Formação em Contexto Militar: Modelos, Processos e Procedimentos
Coordenadores: Tenente-coronel Nuno Alberto Rodrigues Santos Loureiro
Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

32 – A Campanha Militar Terrestre no Teatro de Operações da Guiné-Bissau (1963-1974). Estudo da Aplicação da Força por Funções de Combate
Coordenadores: Brigadeiro-general Jorge Manuel Barreiro Saramago
Tenente-coronel de Administração Domingos Manuel Lameira Lopes

33 – O Direito Português do Mar: Perspetivas para o Séc. XXI
Coordenadora: Professora Doutora Marta Chantal Ribeiro

8 – Orientações Metodológicas para a elaboração de Trabalhos de Investigação (2.ª edição, revista e atualizada)
Coordenadores: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos
Coronel Técnico de Manutenção de Material Aéreo Joaquim Vale Lima

34 – Coreia no Século XXI: Uma península global
Coordenadores: Professora Doutora Teresa Ferreira Rodrigues
Tenente-coronel Rui Jorge Roma Pais dos Santos

35 – O "Grande Médio Oriente" Alargado (Volume I)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Ricardo Dias Costa

36 – O "Grande Médio Oriente" Alargado (Volume II)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Ricardo Dias Costa

37 – As Forças Armadas no Sistema de Gestão Integrada de Fogos Rurais
Coordenador: Tenente-coronel Rui Jorge Roma Pais dos Santos

38 – A Participação do Exército em Forças Nacionais Destacas: Casos do Kosovo, Afeganistão e República Centro-Africana. Vertente Operacional e Logística
Coordenadores: Brigadeiro-general Jorge Manuel Barreiro Saramago
Major de Transmissões Luís Alves Batista
Major de Material Tiago José Moura da Costa

39 – Pensar a Segurança e a Defesa Europeia. Atas do Seminário de 09 de maio de 2019
Coordenador: Tenente-coronel Marco António Ferreira da Cruz

40 – Os Desafios do Recrutamento nas Forças Armadas Portuguesas. O Caso dos Militares Contratados
Coordenador: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

41 – Inovação na Gestão de Recursos Humanos nas Forças Armadas Portuguesas: Os Militares em Regime de Contrato. Atas das Comunicações do *Workshop* de 28 de janeiro de 2019
Coordenador: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

42 – Sistemas de Controlo de Gestão: Modelos, Processos e Procedimentos
Coordenador: Tenente-coronel Nuno Alberto Rodrigues Santos Loureiro

43 – Desafios Estratégicos para Portugal no Pós-Covid-19
Auditores Nacionais do Curso de Promoção a Oficial General 2019/2020

44 – Gestão Estratégica: Contributos para o Paradigma Estrutural da Marinha Portuguesa
Capitão-de-mar-e-guerra Nuno Sardinha Monteiro

45 – A Geopolítica dos *Chokepoints* e das *Shatterbelts* (Volume I)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Marco António Ferreira da Cruz

46 – A Geopolítica dos *Chokepoints* e das *Shatterbelts* (Volume II)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Marco António Ferreira da Cruz

47 – A Geopolítica dos *Chokepoints* e das *Shatterbelts* (Volume III)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Marco António Ferreira da Cruz

48 – Estudos Estratégicos das Crises e dos Conflitos Armados
Coordenadores: Brigadeiro-general Lemos Pires
Tenente-coronel Ferreira da Cruz
Tenente-coronel Pinto Correia
Tenente-coronel Bretes Amador

49 – A Vulnerabilidade em Infraestruturas Críticas: Um Modelo de Análise
Tenente-coronel Santos Ferreira

50 – Função de Combate Proteção
Coordenadores: Coronel de Infantaria Paulo Jorge Varela Curro
Major de Cavalaria Rui Miguel Pinho Silva

51 – Estudos Estratégicos das Crises e dos Conflitos Armados
Coordenadores: Coronel de Cavalaria (Reformado) Marquês Silva
Tenente-coronel GNR Marco Cruz
Tenente-coronel ENGEL Silva Costa
Major Engenheiro Reis Bento

52 – Reinventar as Organizações Militares
Coordenador: Tenente-coronel de Administração Militar Carriço Pinheiro

53 – Estudos de Reflexão sobre as Informações Militares
Coordenador: Tenente-coronel de Infantaria Carlos Marques da Silva

54 – Convulsões Eurasiáticas. *in illo tempore* e agora
Coordenador: Coronel (Reformado) Carlos Manuel Mendes Dias

55 – Estratégias Marítimas – Uma Análise Comparativa (NATO, UE, Espanha, França, Itália, Portugal e Reino Unido)
Coordenadora: Capitão-tenente Sofia Saldanha Junceiro

56 – Ensino e Formação, Avaliação de Desempenho e Retenção do Talento: Dimensões para o Desenvolvimento da Liderança
Coordenador: Tenente-coronel Nuno Alberto Rodrigues Santos Loureiro

57 – Ameaças Híbridas - Desafios para Portugal
Coordenador: Tenente-coronel de Artilharia Diogo Lourenço Serrão

58 – Cadernos de Saúde Militar e Medicina Operacional – Vol. I
Coordenadores: Coronel (REF) António Correia
Primeiro-tenente Nicole Esteves Fernandes

59 – Military Operations in Cyberspace
Coordinator: Lieutenant-colonel João Paulo Ferreira Lourenço

Editorial: cidium@ium.pt
Telefone: (+351) 213 002 100; Fax: (+351) 213 002 162
Morada: Rua de Pedrouços - 1449-027 Lisboa