Can Cyber Operations Directed Against Electrical Infrastructure Be Considered War Crimes Under Article 8 of the Rome Statute? Special Insights from the Russo-Ukrainian War

By

Alexia Collot d'Escury Ariza

ABSTRACT

To determine whether cyber operations directed against electrical infrastructure can be considered war crimes, the Russo-Ukrainian conflict offers a practical application of theoretical debates. Notably, it is investigated whether state actors can face individual criminal responsibility under the Rome Statute for launching cyber attacks against Ukraine's power grid and infrastructure, which was also the target of conventional kinetic strikes.

First, although cyber operations are governed by the principles of International Humanitarian Law, for criminal responsibility to be engaged under Article 8 of the Rome Statute, they must amount to "*attacks*", defined as "*acts of violence*". Cyber attacks are not violent weapons. However, in effect, they cause violent consequences. Whereas destructive cyber operations generate similar effects to kinetic strikes, and thus can qualify as attacks, disruptive cyber operations against electrical systems will only be encompassed if the reverberating effects of electricity disruption on civilians are accounted for, and these effects are harmful.

Second, for a case investigating cyber operations against electrical systems to be admissible before the International Criminal Court (ICC), they must lead to sufficiently grave situations. To this end, they must display sufficient scale in attack, and thus impact. Furthermore, state hackers may not always be the ones who are most responsible for ensuing war crimes, in comparison to superior military commanders. Finally, attacks against electrical systems can constitute war crimes if they are widespread and indiscriminate, qualifying as an attack against civilian objects and/or a violation of the principle of proportionality. This observation is independent of whether the cyber operations were launched alone, or in conjunction with kinetic weapons. However, the strength of this statement will be directly correlated to the benchmarks which the ICC applies to the assessment of targeting electricity.

Last, the war has uncovered gaps in existing law, endowing the ICC with an interpretative role before it can proceed to establishing a case. Notably, the

prohibition of analogy entails that the Court will need to clarify whether cyber operations can be encompassed by the Rome Statute without necessitating amendment. Furthermore, the Court will need to determine the applicable benchmark for analysing the legality of targeting electrical systems, and address their changing role in modern warfare.

TABLE OF CONTENTS

BACKGROUND

Electrical systems have been the object of military operations since the First World War.[1] However the security of the energy sector has long been classified as vital, given that it powers every other critical infrastructure system, and therefore the security dogmas have shifted to encompass cybersecurity threats as well.[2]

On April 8th, 2022, Unit 74455 of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (hereinafter, GRU) launched malwares Industroyer2 and CaddyWiper against a regional Ukrainian energy provider. The cyber attack, however, was successfully detected whilst in progress.[3] Then, on October 6th, 2022, the very same unit launched a successful cyber attack on the Ukrainian power grid. Simultaneously, missiles struck against critical infrastructure across the country.[4] More recently, on September 4th, 2023, Unit 26165 directed malware against a critical energy infrastructure in Ukraine, although it was intercepted.[5]

Unit 26165, also named APT28, Fancy Bear, STRONTIUM, or Forest Blizzard,[6] is classified as an advanced persistent threat.[7] It has been known to

[1] *E.g.*, James W. Crawford III, *The Law of Noncombatant Immunity and the Targeting of National Electric Power Systems* 101 (1997), Fletcher Forum of World Affairs, https://dl.tufts.edu/downloads/xp68ks762?filename=ht24wv85w.pdf.

[2] *See generally*, Cybersecurity & Infrastructure Security Agency, *Energy Systems*, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn/energy (last visited Aug. 8, 2024); European Commission, *Critical infrastructure and cybersecurity*, https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en (last visited Aug. 8, 2024).

[3] ESET Research, *Industroyer2: Industroyer reloaded* (Apr. 12, 2022), https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

[4] Andy Greenberg, *Sandworm Hackers Caused Another Blackout in Ukraine - During a Missile Strike,* Wired (Nov. 9, 2023), https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/.

[5] Anna Ribeiro, *Ukraine's CERT discloses cyberattack on critical energy infrastructure by APT28 hacker group*, Industrial Cyber (Sept. 6, 2023), https://industrialcyber.co/industrial-cyber-attacks/ukraines-cert-discloses-cyberattack-on-critical-energy-infrastructure-by-apt28-hacker-group/.

[6] Microsoft, *How Microsoft names threat actors*, https://learn.microsoft.com/en-us/defender-xdr/microsoft-threat-actor-naming?view=o365-worldwide (last visited Aug. 8, 2024).

[7] FireEye, *APT28: A Window into Russia's Cyber Espionage Operations?* 3 (2014), https://services.google.com/fh/files/misc/apt28-window-russia-cyber-espionage-operations.pdf.

attack high-value targets in various countries,[8] such as the German Bundestag,[9] the Bank of Africa,[10] the White House,[11] or the French President Emmanuel Macron's 2017 election campaign.[12] Unit 74455 is also more commonly known as Sandworm, Seashell Blizzard or IRIDIUM.[13] It is responsible for the 2017 NotPetya malware[14] and the country-wide cyber attacks in Georgia,[15] to name a few. Most notably, it had already triggered blackouts in 2015 and 2016 in Ukraine.[16]

Russian attacks against Ukrainian electrical systems have called into question, first, the status of energy provision vis-à-vis the victims of armed conflicts and, second, the responsibility of state actors who launch operations through cyber means. President of the European Commission, Ursula von der Leyen, tweeted: "*Russia's attacks against civilian infrastructure, especially electricity, are war crimes.*".[17] The aforementioned attacks have encompassed both traditional kinetic force and the launching of cyber operations. Victor Zhora, Chief Digital Transformation Officer at the Ukrainian government's Special

[8] Emil Sayegh, *APT 28 Aka Fancy Bear: A Familiar Foe By Many Names*, Forbes (February 28th, 2023), https://www.forbes.com/sites/emilsayegh/2023/02/28/apt28-aka-fancy-bear-a-familiar-foe-by-many-names/.
[9] Reuters, *Germany Issues Arrest Warrant For Russian Suspect in Parliament Hack: Newspaper* (May 5, 2020), https://web.archive.org/web/20200505153531/https://www.nytimes.com/reuters/2020/05/05/world/europe/05reuters-russia-germany-warrant.html.
[10] Danielle Walker, *APT28 orchestrated attacks against global banking sector, firm finds*, SC Magazine US (May 13, 2015), https://web.archive.org/web/20180302225332/https://www.scmagazine.com/apt28-orchestrated-attacks-against-global-banking-sector-firm-finds/printarticle/414586/.
[11] Cory Doctorow, *Spear phishers with suspected ties to Russian government spoof fake EFF domain, attack White House,* Boing Boing (Aug. 28, 2015), https://boingboing.net/2015/08/28/spear-phishers-with-suspected.html.
[12] Eric Auchard, *Macron campaign was target of cyber attacks by spy-linked group*, Reuters (April 24th, 2017), https://www.reuters.com/article/us-france-election-macron-cyber-idUSKBN17Q200/
[13] Microsoft, *supra* note 6.
[14] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[15] Przemysław Roguski, *Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace*, Just Security (Mar. 6, 2020), https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.
[16] Alex Hern, *Ukrainian blackout caused by hackers that attacked media company, researchers say*, The Guardian (Jan. 7, 2016), https://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company.
[17] Ursula Von der Leyen, X (Oct. 19, 2022, 9:10 AM), https://x.com/vonderleyen/status/1582630271287021570?lang=en.

Communication and Information Protection Service, testified that there is "*some coordination between kinetic strikes and cyber attacks"*, therefore kinetic strikes' "s*upportive actions in cyber can be considered war crimes''* as well.[18]

[18] Shannon Van Sant, *Kyiv argues Russian cyberattacks could be war crimes,* Politico (Jan. 9, 2023, 4:00 AM), https://www.politico.eu/article/victor-zhora-ukraine-russia-cyberattack-infrastructure-war-crime/.

LITERATURE REVIEW AND METHODOLOGY

First, the applicability of the norms of International Humanitarian Law (hereinafter, IHL) to cyber operations (hereinafter, COs) has been extensively researched. Recognised authorities, such as the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (hereinafter, Tallinn Manual 2.0), and the International Committee of the Red Cross (hereinafter, ICRC), have explored it. However, whether COs can fall within the definition of "*attack*" in accordance with Article 8 of the Rome Statute (hereinafter, RS), has not been dealt with directly by these practitioners and, where few academics have discussed it, the debate remains unsettled. Moreover, no Paper has dedicated its study to the specificities of electrical systems in this regard.

Second, whether COs can give rise to sufficiently grave situations to warrant investigation, and prosecution, by the International Criminal Court (hereinafter, ICC), has been explored by academics such as Marco Roscini[19] and Kai Ambos.[20] Command responsibility has specifically been explored as well, for instance in the Tallinn Manual 2.0. Again however, no Paper has yet analysed this from the specific viewpoint of COs targeting electrical systems. Furthermore, the legality of attacking electrical systems has been extensively analysed in relation to past conflicts, such as Iraq or Kosovo. However, the Russo-Ukrainian War has sparked the emergence of academia exploring whether

[19] Marco Roscini has published widely in the field of international law. He is the author of three monographs: *Le zone denuclearizzate* (Nuclear weapon-free zones, Giappichelli 2003), *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) and *International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles* (Oxford University Press 2024). He is also the co-editor of *Non-proliferation Law as a Special Regime* (Cambridge University Press 2012) and the author of several articles and chapters in important international peer-reviewed journals and edited books. Amongst other positions, Roscini is the Swiss Chair of International Humanitarian Law at the Geneva Academy of International Humanitarian Law and Human Rights.

[20] Kai Ambos centres his research on criminal law and procedure, comparative law, and international criminal law. He has various publications in these areas, and his most recent ones include: *Commentary of the Rome Statute of the International Criminal Court* (Beck/Nomos/Hart 2022), Treatise of International Criminal Law (Oxford 2013-2016), *The Crime of Genocide and the Principle of Legality under Article 7 of the European Convention on Human Rights* (Human Rights Law Review 2017). Amongst other positions, Ambos acts as a Judge at the Kosovo Specialist Chambers in the Hague, Acting Director of the Institute for Criminal Law and Justice, and Advisor (*Amicus Curiae)* to the Colombian Special Jurisdiction for Peace.

widespread attacks against electrical systems can constitute war crimes, notably commented on by Michael N. Schmitt[21] and Charles J. Dunlap Jr.[22] Nevertheless, the studies are limited in their scope, and do not address the particularities of the participation of COs in the attacks.

Finally, whether the prohibition of analogy may impede the Rome Statute from encompassing COs in future prosecution has been very rarely explored by academia, citing here the work of Jennifer Trahan[23] and Roscini. The war has sparked debates on whether the text needs amendment, but the study is recent and incomplete. Furthermore, calls for revising the applicable assessments to targeting electricity systems have been made, yet very few academics, one being Francesca Capone,[24] have yet to assess it as well.

This Paper therefore presents an original take on the future of international criminal responsibility in the face of modern warfare tactics. It conjunctly analyses the potential criminal responsibility of individuals launching COs, which has been limitedly explored (Ambos, in his study of the matter, denotes the existence of very few academia, with the Tallinn Manual 2.0 only

[21] Michael N. Schmitt is a prolific scholar in the study of international humanitarian law, the use of force, and the international law applicable to cyber operations. He is internationally known for his work in directing the two Tallinn Manuals [cited above]. Amongst other positions, Schmitt is the G. Norman Lieber Distinguished Scholar at the Lieber Institute of the United States Military Academy (West Point), the Charles H. Stockton Distinguished Scholar in Residence at the US Naval War College, and serves as General Editor of Oxford University Press' Lieber Studies series. He is the author of more than 200 scholarly publications.

[22] Charles J. Dunlap Jr. totals more than 120 publications addressing a wide range of issues, including national security, the law of armed conflict, the use of force under international law, civil-military relations, cyberwar, airpower, military justice, and ethical issues related to the practice of national security law. Major General Dunlap retired from the Air Force in 2010, having most notably served as Deputy Judge Advocate General of the United States Army from 2006 to 2010. He is now a Professor of Law at Duke Law faculty.

[23] Jennifer Trahan is an internationally renowned expert on issues of international law and international justice. Amongst other notable positions, she serves as one of the US representatives to the Use of Force Committee of the International Law Association, and has served as an *amicus curiae* to the International Criminal Court on the appeal of the situation regarding Afghanistan, and on the Council of Advisers on the Application of the Rome Statute to Cyberwarfare. Her recent book, *Legal Limits to Security Council Veto Power in the Face of Atrocity Crimes* (Cambridge U. Press 2020), received the 2020 Book of the Year Award from the American Branch of the International Law Association.

[24] Francesa Capone has undertaken research on a wide range of topics, encompassing the law of remedies, the legal framework governing the response to CBRN events and the issues connected to international law and terrorism. She has been a visiting fellow and guest lecturer at several academic institutions across Europe, including Leiden University and the Max Planck Institute for Comparative Public Law and International Law.

dedicating two out of one hundred and fifty four rules to it), and the revised view on the status of electricity systems, only newly emerging, in a practical review. Where research exists in a particular field, or prosecutorial step, it has not analysed the two points of contention together. Furthermore, findings are rarely applied to studying existing hacks. Thus, this Paper proposes an approach to constructing a successful prosecutorial process.

The Russo-Ukrainian War represents a unique opportunity to determine if the International Criminal Court could launch a successful investigation into, and prosecution of, those individuals responsible for launching cyber attacks against Ukraine's national energy grid. By applying legal theory to a case study, this Paper ultimately aims to determine whether cyber operations launched against electrical infrastructure can be considered war crimes under Article 8 of the Rome Statute. This investigation will be carried out in three Chapters, firstly ascertaining how the principles of *Jus in Bello* apply to cyber operations, secondly establishing whether attacks against electrical systems can be considered war crimes, and finally discerning what the war has underscored in regards to the ICC's role, and future obstacles, in addressing such crimes under the current texts.

To this purpose, this Paper draws on diverse sources for information on the war in Ukraine, including international news outlets like BBC News and The New York Times, specialised security and cybersecurity news reports, such as Mandiant and the Center for Strategic and International Studies, as well as human rights organisations' take, like Amnesty International and the International Rescue Committee. Furthermore, views were extracted from assemblies and press releases of governmental and international bodies, like the ICRC and the United Nations Security Council. It also incorporates statements from officials of the State parties at stake. To supplement this information, this Paper has gathered data from International Databases, like the CyberPeace Institute, and materials for their legal analysis, such as from the ICRC's IHL Databases on Rules and Practice.

AUTHOR'S NOTE

First, this Investigation focuses on the actions and policies of the Russian Government and Military, and it in no way seeks to attribute responsibility to Russian citizens as a nation. Whilst references to "the Russian Federation" or "Russia" appear throughout this Study, they should be understood as referring specifically to the decisions and conduct of the current Russian Government and its Officials exclusively. This distinction is crucial in maintaining an objective and fair analysis, particularly in a context where the actions of a State actor may have to be separated from the broader population which it governs.

Second, the temporal scope of this Investigation is confined to the cyberattacks which were launched by Sandworm and FancyBear against electrical systems in Ukraine up until September 2023, thereby deliberately excluding subsequent developments. For instance, on April 19th 2024, the Computer Emergency Response Team of Ukraine (CERT-UA) released a report declaring that, in March, they had uncovered a malicious plot of the Sandworm group, aimed at disrupting the stable operation of information and communication systems of about twenty energy, water and heating supply enterprises in ten regions. Whilst acknowledging that the latter events undoubtedly impact the broader context of the Investigation, such as by having the potential of shaping the Gravity Analysis contained in Chapter II Part I, it was necessary to establish a defined scope for this Paper to provide a coherent and focused analysis which is representative of the methodology applied by the International Criminal Court. These developments may thus warrant future further examination or inclusion in the considerations of this Study.

CHAPTER I. How do the principles of Jus in Bello apply to cyber operations?

Cyberspace operations, or in short, 'cyber operations', are defined as the "*employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace*".[25] Academia converges in that the principles of *Jus in Bello* govern, and limit, any use of COs by States in the context of an armed conflict.[26] However, the manner in which the existing framework should apply, and whether it is sufficient, remains the subject of controversy.[27] In this Chapter therefore, this Paper aims to, firstly, showcase the existing gap in the normative framework of IHL and, secondly, explore the different manners in which this gap may be filled. Particularly, there is dissent amongst academia and practitioners regarding which type of COs against electrical systems constitute an 'attack' within the meaning of IHL, and therefore fulfil the 'attack' requirement for Art.8 to be engaged. This Chapter will determine that different types of COs directed against electrical infrastructure can rise to the requisite level of 'attack', and therefore trigger international criminal responsibility.

I. The Gap in the Geneva Conventions and its Protocols regarding cyber operations

[25] Committee on National Security Systems, CNSSI No. 4009, *Glossary* (Apr. 6, 2015), https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf.

[26] *E.g.*, NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn manual 2.0 on the international law applicable to cyber operations* 375 (Michael N. Schmitt ed., 2nd ed., 2017) [hereinafter, *Tallinn manual 2.0]*; Kubo Macák & Tilman Rodenhäuser, *Towards common understandings: the application of established IHL principles to cyber operations*, Humanitarian Law & Policy (Mar. 7, 2023), https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/.

[27] International Committee of the Red Cross, *International humanitarian law and cyber operations during armed conflicts ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019*, 102 no. 913 International Review of the Red Cross 481, 482 (2020), doi:10.1017/S1816383120000478.

When an armed conflict erupts, a legal threshold is crossed, and the international laws regulating the conduct of war (IHL, or *Jus in Bello*) are triggered.[28] The normative architecture of IHL is composed of treaties and customary law.[29] To this investigations' purpose, focus will be placed on the provisions of "Protocol Additional to the Geneva Conventions of August 12th, 1949, and relating to the Protection of Victims of International Armed Conflicts" (hereinafter, AP I). Ukraine and the Russian Federation are both parties to it, and thus bound by its obligations, although the latter withdrew its acceptance of the competence of the International Fact-Finding Commission in 2019.[30]

Cyber activities are not expressly regulated by the existing legal framework.[31] Yet, it is presumed that IHL applies to COs,[32] because "*the law of armed conflict [...] applies to all forms of warfare and to all kinds of weapons, those of the past, present, and future*".[33] In effect, the United Nations' Group of Governmental Experts has already concluded that international law including, where applicable, the principles of humanity, necessity, proportionality, and distinction, apply to the use of ICTs by States.[34] Accordingly, attacks against civilians and civilian objects, disproportionate attacks, and attacking, destroying, removing, or rendering useless objects indispensable to the survival of the civilian population, are prohibited, including when using cyber means of warfare.[35] Such conduct may therefore qualify as war crimes.[36]

---

[28] Eliav Lieblich, *The Facilitative Function of Jus in Bello*, 30 no. 1 The European Journal of International Law 321, 322 (2019), doi:10.1093/ejil/chz015.
[29] Michael N. Schmitt, *Normative architecture and applied international humanitarian law*, 104 no. 920-21 International Review of the Red Cross 2097, 2098 (2022), doi:10.1017/S1816383122000662.
[30] Ministry of Foreign Affairs of the Russian Federation Press Release, *Press release on the withdrawal of the declaration to Protocol Additional to the 1949 Geneva Conventions and relating to the protection of victims of international armed conflicts (Protocol I) on Russia's acceptance of the competence of the International Fact-Finding Commission* (Oct. 22, 2019 6:41 PM), https://www.mid.ru/en/foreign_policy/news/1473198/.
[31] Tallinn manual 2.0, *supra* note 26.
[32] International Committee of the Red Cross, *supra* note 27 at 485.
[33] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 95, ¶ 86 (July 8).
[34] U.N. GAOR 70th Sess., Item 93 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, at 3, U.N. Docs. A/70/174 (22 July, 2015).
[35] International Committee of the Red Cross, *supra* note 27 at 486-7.
[36] Tallinn manual 2.0, *supra* note 26 at 392.

II. Applicability of IHL by analogy

The war in Ukraine, and prominently the Russian attacks against the energy grid, have displayed a deployment of cyber capabilities in conjunction with conventional forces, thus amongst other possible references, a 'cyber-enabled warfare'.[37] In return COs encompass, inter alia, cyber espionage, cyber manipulation, and cyber attacks,[38] the latter being the strongest, most aggressive form of CO.[39] Notably, the COs which were launched by Fancy Bear and Sandworm against Ukraine's energy grid fall into the latter category.[40]

IHL provides specific protections regardless of the type of harmful operation.[41] For example, it is prohibited to make unauthorised use of the distinctive emblem of the United Nations, including in any type of cyber operation.[42] However military operations, including COs, must meet a requisite threshold to be encompassed by some of the norms of *Jus in Bello*, that is, they must qualify as "*attacks*" under IHL.[43] Although it will be explored in Chapter II, it may be advanced here that the accusations levied against the Russian Federation for targeting Ukrainian electrical systems encompass the prohibition of "attack[ing]" civilians[44] and civilian objects,[45] as well as the prohibition of carrying out disproportionate "attacks".[46] Therefore, for a CO to breach the norms of *Jus in Bello,* and engage responsibility under the specified provisions of the RS, it must first of all be an 'attack'. The latter was not defined in the RS, however Art. 49 AP I delineates them as "*acts of violence against the adversary*".

[37] Trey Herr & Drew Herrick, *Military Cyber Operations: A Primer*, no. 14 The American Foreign Policy Council Defense Technology Program Brief 1, 1 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2725275.
[38] Kai Ambos, *Cyber-Attacks as International Crimes under the Rome Statute of the International Criminal Court?*, *in* Cyber Operations and Cyberwarfare Question *in* ICCForum (Mar. 7, 2022), https://iccforum.com/cyberwar.
[39] *Id.*
[40] CyberPeace Institute, *Energy*, *in* Impact & Harm: Sectors, *in* Cyber Attacks in Times of Conflict Platform #Ukraine (last visited Aug. 10, 2024), https://cyberconflicts.cyberpeaceinstitute.org/impact/sectors/energy.
[41] International Committee of the Red Cross, *supra* note 27 at 489.
[42] Art.38(2) AP I; *See also* Tallinn manual 2.0, *supra* note 26 at 99.
[43] International Committee of the Red Cross, *supra* note 27 at 489.
[44] Art.51(2) AP I and Art.8(2)(b)(i) RS.
[45] Art.52(1) AP I and Art.8(2)(b)(ii) RS.
[46] Art.51(5)(b) AP I and Art.8(2)(b)(iv) RS.

A. Can COs be termed "acts of violence"?

The plain text of Article 49 appears to require a 'violent act' for qualification of conduct as an 'attack'. Therefore non-kinetic operations, by strict textual interpretation, would be excluded.[47] This follows from the means-based approach to the definition, which focuses on the instrument used,[48] and thus poses a difficulty for COs in general to qualify as 'attacks'.[49]

However, there exist precedents advocating for IHL to limit certain actions due to their violent consequences, even without a conventional manifestation of physical force.[50] For example, IHL limited the use of chemical and biological weapons.[51] It is in fact consistent with the law of armed conflict's underlying humanitarian purposes to adapt its interpretation of 'attack' to encompass new kinds of weapons which negatively impact the safeguards afforded by AP I,[52] falling in line with the ICRC's reiterated concern regarding the humanitarian consequences of cyber-enabled warfare.[53] This in return stems from the contrasting approach, which is effects-based.[54] The latter has gained the most support amongst the international community, including by the ICRC,[55] and in the Tallinn Manual 2.0, thereby centering on the violent consequences, or the ensuing damage [of COs], and not on violent acts *per se*.[56] Therefore, COs in

[47] Michael N. Schmitt, *Cyber Operations and the Jus In Bello: Key Issues,* 87 International Law Studies 89, 93 (Raul P. Pedrozo & Daria P. Wollschlaeger eds., 2011), https://digital-commons.usnwc.edu/ils/vol87/iss1/7/.
[48] Kai Ambos, *International Criminal Responsibility in Cyberspace, in* Research Handbook on Cyberspace and International Law 122 (Nicholas Tsagourias & Russel Buchan eds., 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412626.
[49] David Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, 22 University of Minnesota Law School 347, 365 (2013), https://scholarship.law.umn.edu/faculty_articles/223/.
[50] Ido Kilovaty, *Virtual Violence - Disruptive Cyberspace Operations as "Attacks" Under International Humanitarian Law* 23 no. 1 Michigan Telecommunications and Technology Law Review 113, 118 (2016), https://repository.law.umich.edu/mttlr/vol23/iss1/3.
[51] Geneva Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925.
[52] Tallinn manual 2.0, *supra* note 26 at 417.
[53] U.N. GAOR 66th Sess., Items 87 & 106 *General Debate on All Disarmament and International Security Agenda Items*, 1st Comm'n, Statement by the Int'l Comm. of the Red Cross (Oct, 2011).
[54] David Weissbrodt, *supra* note 49.
[55] International Committee of the Red Cross, *supra* note 27 at 489.
[56] Tallinn manual 2.0, *supra* note 26 at 415.

general may be viewed as 'acts of violence', if they cause the requisite damage or consequence.

B. Can COs targeting electrical infrastructure give rise to "violent consequences" or "damage"?

COs, or in this case, cyber attacks, against electrical infrastructure, cause three types of consequences in the physical world: primary, secondary, and tertiary. The primary effects regard the impact which the CO has on the information system operating the grid or infrastructure (hereinafter, IT). Secondary effects then refer to the impact on the grid or infrastructure itself. Finally, the tertiary effects encompass the repercussions for the population who relies on the targeted grid or infrastructure.[57] Destructive COs, like Sandworm's April 2022 attempt,[58] overwrite, erase, or physically destroy information so that it cannot be recovered.[59] This implies, thus, a directly destructive effect or violent consequence for the object, the damage to the IT system.[60] This is akin to the physical outcome which a kinetic military attack would have had.[61] A destructive cyber attack against the IT of an electrical system thus qualifies as an 'attack' within the meaning of Art.49 AP I.

However, disruptive COs, such as Sandworm's October 2022 cyber attack, solely cause the energy grid or infrastructure to be inoperable for a length of time.[62] There is therefore no directly destructive, primary effect on the IT

[57] National Research Council of the National Academics, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* 80 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009), https://nap.nationalacademies.org/read/12651/chapter/1.
[58] CyberPeace Institute, *supra* note 40.
[59] Elaine Barker & William C. Barker, *NIST Special Publication 800-57 Part 2 Revision 1, Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations* 9 (May, 2019), https://doi.org/10.6028/NIST.SP.800-57pt2r1.
[60] Tallinn manual 2.0, *supra* note 26 at 415.
[61] Georgia Beatty, *War crimes in cyberspace: prosecuting disruptive cyber operations under Article 8 of the Rome Statute* 58 no. 2 The Military Law and the Law of War Review 209, 212 (Dec., 2020), https://doi.org/10.4337/mllwr.2020.02.17.
[62] Marianne Swanson et al., *NIST Special Publication 800-34 Rev. 1. Contingency planning guide for federal information systems* app. G-1 (May 2010), http://dx.doi.org/10.6028/nist.sp.800-34r1.

system. Hence, experts have debated whether disruptive cyber operations (hereinafter, DCOs) can be deemed 'attacks' for the purposes of IHL.[63]

Should an overly physical approach to the assessment of 'violent consequences' or 'damage' be taken, the qualification of DCOs as 'attacks' would prove difficult.[64] A majority of the Experts who make up the working group responsible for the Tallinn Manual 2.0 were of the opinion that interference with the functionality of an electrical system qualifies as damage if restoration of functionality of the grid or infrastructure requires replacement of physical components. Some of the Experts in this majority further held that the notion of damage extends to situations in which reinstallation of the operating system or of particular data is required in order to regain functionality.[65] Whether Sandworm's October 2022 DCO, or Fancy Bear's September 2023 attempted malware launch, entailed such reparative needs has not been disclosed.

However, classifying destructive COs as 'attacks' due to their kinetic effect creates a 'kinetic effect equivalence' requirement which would exclude DCOs from the definition. This analysis has been challenged in that a 'true' effects-based approach would extend the notion of 'violent consequence' or 'damage' to the harm suffered by the population as a result of electricity disruption,[66] that is, the tertiary effect.

The ICRC and the Tallinn Manual 2.0 have both determined that the analysis of 'consequential violence' does not halt at the primary (IT impact), or secondary (infrastructure impact) effect, but in fact also encompasses any reasonably foreseeable consequential damage, destruction, injury or death (indirect or reverberating effects).[67] Therefore, DCOs targeting electrical systems which are expected to cause this result constitute 'attacks' under IHL.[68] More precisely, according to the ICRC, the foreseeable harm falling within the

[63] Ido Kilovaty, supra note 50.
[64] Georgia Beatty, *supra* note 61 at 229.
[65] Tallinn manual 2.0, *supra* note 26 at 417.
[66] Georgia Beatty, *supra* note 61 at 233.
[67] Tallinn manual 2.0, *supra* note 26 at 416.
[68] International Committee of the Red Cross, *supra* note 27 at 489.

definition of Art.49 AP I extends for example to the death of hospital patients caused by a DCO on an electricity network that results in cutting off the hospital's supply.[69] The October 2022 Sandworm DCO may therefore be deemed an 'attack' under this lens, if and it may be presumed, the blackouts it contributed to impacted the livelihood of civilians, thus generating the requisite degree of 'consequential violence'. For instance, by October 20th, 2022, 40% of Ukraine's energy facilities had been damaged,[70] leaving 4.000 settlements in 11 regions without electricity, including for water and medical assistance purposes.[71]

Further encompassing, according to the Deputy Head of the Legal Division at the ICRC, Knut Dörmann, and as was supported by a minority of the Experts of the Tallinn Manual 2.0, the loss of usability of the grid or infrastructure in itself constitutes sufficient 'damage' (the secondary effect).[72] According to this position, allowing a DCO directed at a civilian network such as electricity to fall outside the scope of IHL, just because it is reversible or does not cause structural damage, is an overly restrictive definition of 'attack', difficult to reconcile with the humanitarian purposes of *Jus in Bello*.[73] Some academics have deemed this more extreme alternative to be plausible, for it responds to concerns that the kinetic-equivalence approach, followed by most of the Experts in the Tallinn Manual, is under-inclusive.[74] Under this lens, any of the GRU's COs against electrical systems would constitute an 'attack' because the required threshold of 'consequential violence' would be reached already at the production of the

[69] *Id.*
[70] Amnesty International, *Ukraine: Russian attacks on critical energy infrastructure amount to war crimes* (Oct. 20, 2022), https://www.amnesty.org/en/latest/news/2022/10/ukraine-russian-attacks-on-critical-energy-infrastructure-amount-to-war-crimes/.
[71] Hugo Bachega & Yaroslav Lukov, *Ukraine war: Blackouts in 1,162 towns and villages after Russia strikes*, BBC (Oct. 18, 2022), https://www.bbc.com/news/world-europe-63297239.
[72] *See* Ido Kilovaty, *supra* note 50; *Accord* Tallinn manual 2.0, *supra* note 26 at 418.
[73] *See* Knut Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks*, International Committee of the Red Cross, 4 (2004), https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/applicabilityofihltocna.pdf ; *Accord* International Committee of the Red Cross, *International Humanitarian Law and cyber operations during armed conflict, ICRC position paper*, 8 (Nov., 2019), https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf.
[74] Georgia Beatty, *supra* note 61 at 233.

secondary effect, the disruption, or attempted disruption, of electricity. On the other hand, foregoing the analysis of the tertiary effect may render the approach over-inclusive, allowing DCOs of which the impact is mere inconvenience to constitute an 'attack'.[75]

Finally COs, including DCOs, which unsuccessfully target electrical systems may be deemed 'attacks'. Indeed an attack that is successfully intercepted and does not result in actual damage is still an 'attack' under IHL, if it would have been likely to cause the requisite 'violent consequence'. The same applies to cyber attacks.[76] The April 2022 Sandworm destructive attack was halted, therefore it did not actually cause the requisite primary 'violent consequence' or 'damage' to the IT system. However, it was likely to,[77] and this is sufficient. Furthermore, if the tertiary effect is taken account of, it also rises to the level of 'attack'. According to Farid Safarov, Ukraine's Deputy Minister of Energy, the cyber attack was expected to impact an area where more than two million Ukrainians live.[78] Regarding the September 2023, attempted malware launch, no information has been disclosed by the authorities on the targeted infrastructure.[79] Therefore it cannot be assessed if, in primary effect, it would have been destructive, or if in reverberating effect, it would have led to injury or death. However, some sources describe the facility as critical,[80] which potentially indicates that the tertiary impact would have been significant.

[75] Michael N. Schmitt, *supra* note 47 at 104.
[76] Tallinn manual 2.0, *supra* note 26 at 419.
[77] Andy Greenberg, *Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine*, Wired (Apr. 12, 2022 10:44 AM), https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/.
[78] Sean Lyngaas, *Russian military-linked hackers target Ukrainian power company, investigators say*, CNN (Apr. 14, 2022, 11:04 AM), https://edition.cnn.com/2022/04/12/politics/gru-russia-hackers-ukraine-power-grid/index.html.
[79] Computer Emergency Response Team of Ukraine, *Кібератака APT28: msedge як завантажувач, TOR та сервіси mockbin.org/website.hook як центр управління (CERT-UA#7469)* [APT28 cyberattack: msedge as a downloader, TOR and mockbin.org/website.hook services as a control centre (CERT-UA#7469)], Gov. Ukr. (Sept. 4, 2023), https://cert.gov.ua/article/5702579?fbclid=IwAR3XlwoRXJ793jQf96FKqvcTE6rgQtQri--9_QnzH70ceeJtE2w6OcPxL-g.
[80] Kevin Poireault, *Russia-Backed APT28 Tried to Attack a Ukrainian Critical Power Facility*, InfoSecurity Magazine (Sept. 6, 2023), https://www.infosecurity-magazine.com/news/russia-apt28-attack-ukraine-power/.

III. Partial Conclusion

There are many challenges to COs being deemed 'acts of violence' for the purposes of the definition of 'attack' under IHL, and therefore to engage individual criminal responsibility under Art.8 RS. Even if the effects-based approach is followed, and 'violent consequences' are taken into account as opposed to instrumentality, COs targeting electrical systems pose a particular interpretative obstacle. Accordingly, if the 'kinetic-equivalence approach' is followed, only destructive COs may qualify as 'attacks'. Although this position has been criticised, and it has been deemed that DCOs should also be viewed as 'attacks' precisely because the disruption of electricity has a tertiary 'violent consequence' for civilians, again dissenting theories emerged amongst academia and practitioners. Therefore, even if COs are deemed 'attacks' by analogy, it may be that not all types of COs targeting electrical systems can be encompassed by the state of the normative framework, evidencing the existing gaps in IHL. Such a debate on the extent of civilian harm to be accounted for when considering the particular case of operations against electrical systems will be explored in further detail, and thereby brings us to Chapter II.

CHAPTER II. Can attacks against electrical infrastructure be considered war crimes?

Even when a CO targeting electrical systems amounts to an 'attack' within the meaning of Art.8 RS, it is yet to be determined whether the operation in question is encompassed by the prohibitions of Art.8. On admissibility, it must be ascertained whether COs targeting electrical systems can give rise to sufficiently grave situations to warrant investigation, and prosecution, by the Office of The Prosecutor (hereinafter, OTP). Thereafter, it must be established whether such attacks can constitute war crimes for the purposes of establishing the subject-matter jurisdiction of the Court. Hereby, academics and practitioners disagree on the applicable theories and interpretations. First, it is not clear whether in scale, nature, manner of commission, or impact, COs, and specifically those targeting electrical systems, can give rise to sufficiently grave situations. Second, debates arise in regards to whether members of hacking teams should be the objects of investigation, and prosecution, or whether their superior military commanders should be deemed 'the most responsible'. Last, the lawfulness of targeting electrical systems has not been settled under international law. Employing the Russo-Ukrainian War as a practical application of theoretical debate, this Chapter will determine that COs targeting electrical installations can give rise to sufficiently grave situations to warrant investigation into those 'most responsible' for the attack, and as well, engage the subject-matter jurisdiction of the Court as a war crime.

I. Do cyber attacks against electrical systems give rise to sufficiently grave situations for the ICC to investigate, and prosecute, alleged war crimes?

Gravity is an element of the crimes in the RS.[81] Art.5 refers to "*the most serious crimes of concern to the international community*". Regarding the alleged

[81] Art. 17(1)(d) & Art.53 RS.

war crimes of interest to this Paper, Art.8(2)(b) refers to "*serious violations*". Additionally, gravity constitutes a non-discretionary admissibility threshold,[82] referred to as 'legal gravity'.[83] Finally, gravity also guides the discretionary decision of the OTP on the selection and prioritisation of admissible cases to investigate and prosecute, the 'relative gravity'.[84]

According to case law, the assessment is two-fold. The Court carries out a quantitative and qualitative assessment in relation to the nature, scale, manner of commission, and impact, of the alleged crimes, and it examines whether the persons who will likely be the object of investigation and prosecution are the "*most responsible*" for the alleged crimes.[85] COs, particularly when they target electrical infrastructure, pose a particular challenge.

A. Can alleged war crimes targeting electrical systems, perpetrated through cyber means, give rise to sufficiently grave situations?

Regarding the first element of the gravity assessment, doubts arise with respect to whether COs targeting electrical systems are capable of amounting to 'serious violations' within the meaning of Art.8(2)(b) RS.

With respect to the quantitative analysis, that is, 'scale', it inter alia centres on the number of victims, the extent of the damage caused, in particular the bodily or psychological harm, or their geographical or temporal spread.[86] As was already posited in Chapter I, in comparison to traditional kinetic force, COs do not directly cause fatalities or damage. However, again, this analysis may be analogically adapted to encompass injury or death indirectly caused by COs

[82] Marco Roscini, *Gravity in the Statute of the International Criminal Court and cyber conduct that constitutes, instigates or facilitates international crimes,* 30 Criminal Law Forum 247, 253 (2019), https://doi.org/10.1007/s10609-019-09370-0.
[83] *E.g.*, Kai Ambos, *Treatise on International Criminal Law: Volume III: International Criminal Procedure* 292 (2016).
[84] Margaret M. deGuzman, *Gravity and the Legitimacy of the International Criminal Court*, 32 Fordham International Law Journal 1400, 1405 (2009).
[85] *The Prosecutor v. Bahar Idriss Abu Garda,* ICC-02/05-02/09, Decision on the Confirmation of Charges, ¶ 31 (Feb. 8, 2016).
[86] The Office of the Prosecutor ICC, *Policy paper on preliminary examinations* 15 (Nov., 2013), https://www.icc-cpi.int/sites/default/files/iccdocs/otp/OTP-Policy_Paper_Preliminary_Examinations_2013-ENG.pdf.

(tertiary effect). This may hold particularly true in regards to COs which target electrical systems, when they entail the deprivation of electricity to a large sector of the population, and thus ensuing risk to livelihood. For example, it has been proposed that a cyber attack that shuts down an electrical power station in the middle of a harsh winter, with consequent deaths among the civilian population due to the low temperatures, causes significant damage for the purposes of the Court's gravity assessment.[87]

Regarding qualitative factors, 'nature' refers to the specific elements of the offence, such as rape, crimes against children, or notably, the imposition of conditions of life on a group, calculated to bring about its destruction.[88] Psychological suffering may also be taken into account.[89] As regards COs targeting electrical systems, following Title II of this Chapter explores Russia's potential liability under Art.8(2)(b)(xxv), for attempting to cause starvation through long-term and widespread electricity deprivation. It may be advanced that critical services to civilians, such as water pumping, hospital services, and food production, depend on energy to function. Nevertheless, although the argument that there is a hierarchy of crimes has been deemed controversial,[90] the characteristics of COs do not entirely fit the definition of a particularly serious 'nature'. With respect to 'the manner of commission', whilst it is doubtful that ICTs constitute an aggravating factor insofar as the means of execution are concerned,[91] COs targeting electrical systems may evidence a particularly malicious intent when they are specifically carried out during winter time, like Russia did.[92] Elements of cruelty are of significance to this assessment.[93] Finally

[87] Marco Roscini, *supra* note 82 at 261.
[88] The Office of the Prosecutor ICC, *supra* note 86.
[89] *The Prosecutor v. Ahmad Al Faqi Al Mahdi*, ICC-01/12-01/15, Judgment and Sentence, ¶ 78-9 (Sept. 27, 2016).
[90] William A. Schabas, *An introduction to the international criminal court* 81 (June 2020), https://doi.org/10.1017/9781108616157.
[91] Marco Roscini, *supra* note 82 at 266.
[92] Andriy Yermak, *In Ukraine, Russia is trying to freeze us into submission or death. It will fail*, The Guardian (Dec. 1, 2022, 5:00 PM), https://www.theguardian.com/commentisfree/2022/dec/01/ukraine-russia-freeze-power-starvation-holodomor-terror (head of the Ukrainian presidential office, commenting that he feared that Russia was now seeking '*death by freezing*').
[93] The Office of the Prosecutor ICC, *supra* note 86 at 15-6.

regarding 'impact', considered here are, among others, the suffering of the victims, the terror instilled, or the socio-economic damage inflicted on the community.[94] It is generally accepted that COs which target national critical infrastructures like electricity, disrupting the provision of critical services, have a more significant impact on the broader community than those on other infrastructures.[95]

Therefore, although COs targeting electrical systems have the potential to give rise to sufficiently grave situations, their particularities nevertheless pose a challenge. Whereas the legal gravity threshold is not very high,[96] still an isolated cyber attack against protected objects which results in negligible damage and little impact would not cross the threshold.[97] Insofar as the relative gravity threshold is concerned, the OTP applies a stricter test.[98] When individual COs, such as those launched by Sandworm and Fancy Bear, are scrutinised, they run the risk of falling short from this assessment.

However in the context of a cyber-enabled warfare against electrical systems, like in the Russo-Ukrainian conflict, evidence may be found of the existence of a plan or policy within the meaning of Art.8(1) RS: *"the Court shall have jurisdiction in respect of war crimes in particular when committed as part of a plan or policy or as part of a large-scale commission of such crimes"*. Although this will be further explored, it may be underlined that, the day that Sandworm launched its cyber attack, missiles struck critical energy infrastructure across Ukraine.[99] To the day of the writing of this Paper, in early 2024, the strikes have

[94] *Id.* at 16.
[95] Marco Roscini, *supra* note 82 at 268-9.
[96] Ignaz Stegmiller, *The Pre-Investigation Stage of the ICC: Criteria for Situation Selection* 352 (2011), ISBN-13 978-3428133505.
[97] *Id.*
[98] The Office of the Prosecutor ICC, *Policy paper on case selection and prioritisation* 13 (Sept. 15., 2016), https://www.icc-cpi.int/sites/default/files/itemsDocuments/20160915_OTP-Policy_Case-Selection_Eng.pdf.
[99] Mandiant, *Sandworm Disrupts Power in Ukraine Using a Novel Attack against Operational Technology*, Google Cloud (Nov. 9, 2023), https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/?hl=en.

not halted.[100] Although Art.8(1) only constitutes statutory guidance,[101] when COs form part of a cyber-enabled warfare, they may become an integral part of an operation which constitutes an attack,[102] thereby facilitating success under the gravity assessment. For example, a significant geographical and temporal spread for the purposes of the quantitative criterion is then found. Meanwhile, for one or various COs alone to qualify, they would have to evidence a particular great scale in electricity disruption, and thus also impact. Regardless, all of these observations are subject to the assessment being expanded to take into account reverberating effects.

B. Which level of the chain of command should be deemed "most responsible" in relation to crimes perpetrated through cyber means?

A particular challenge arises regarding whether hackers should be the ones bearing responsibility for COs which constitute war crimes, or whether "*military commanders*" or "*other superiors*" should be the ones investigated, and prosecuted.[103] In the *Mavi Marmara* situation, the OTP equated those most responsible with the "*most senior*".[104] However, the Pre-Trial Chamber subsequently ruled that seniority or hierarchy has no bearing on the identification of the individuals 'most responsible'.[105]

On the one hand however, a case may be more effectively established against a 'superior', or 'commander', who plans and orders multiple cyber

[100] *E.g.*, Ukrinform, *Russian missile strike destroys electric substation in Lviv* (Feb. 15, 2024 4:30 PM), https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/?hl=en.
[101] The Office of the Prosecutor, *Situation on Registered Vessels of Comoros, Greece and Cambodia. Article 53(1) Report* (Nov. 6, 2014), https://www.icc-cpi.int/sites/default/files/iccdocs/otp/OTP-COM-Article_53(1)-Report-06Nov2014Eng.pdf.
[102] Tallinn manual 2.0, *supra* note 26 at 420.
[103] Art.28 RS.
[104] *Situation in the Registered Vessels of the Union of the Comoros, the Hellenic Republic of Greece and the Kingdom of Cambodia*, ICC-01/13, Prosecution Response to the Application for Review of its Determination under article 53(1)(b) of the Rome Statute, ¶ 62 (Mar. 30, 2015).
[105] *Situation in the Registered Vessels of the Union of the Comoros, the Hellenic Republic of Greece and the Kingdom of Cambodia*, ICC-01/13, Decision on the request of the Union of the Comoros to review the Prosecutor's decision not to initiate an investigation, ¶ 23 (July 16, 2015).

attacks, than against individual hackers themselves.[106] From this perspective, when COs are launched against energy systems together with kinetic strikes, or when various COs target the same infrastructure or sector, responsibility extends throughout the chain of command or control to subordinate commanders, and superior orders.[107] In practical terms, the argument holds. Sandworm and Fancy Bear are individual Units, themselves part of one of the fifteen directorates which make up the GRU.[108] In cyber-enabled warfare, kinetic and cyber weapons may converge against single targets or sectors like electricity, and this presumption of a common plan or policy in return places the coordinating, higher ranking officials under the investigative lens.[109] Thereby, hypothetically,[110] the head of the GRU Kostyukov Igor,[111] may be 'more responsible' for directing the cyber attacks. Alternatively Sergei Shoigu, General Staff and Defense Minister,[112] may be 'more responsible' for the overall plan since the GRU acts under his command. This proposal is not affected by the fact that a CO fails, as in the case of the April 2022 and September 2023 launches, since responsibility also applies to crimes attempted pursuant to an order.[113]

On the other hand, the fact that hackers may be merely obeying orders does not relieve them of responsibility.[114] Particularly regarding the technical complexity of COs, hackers may have a better understanding of the operation, and should therefore be the ones who are aware of the illegality of the attack.[115] To this extent commanders are allowed to rely on the knowledge of their subordinates.[116] In the Russo-Ukrainian context however, this consideration does

[106] Dan Saxon, *Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare: Challenges for Investigations and Prosecutions*, 21 no. 3 Journal of Conflict and Security Law 555, 564 (2016), https://doi.org/10.1093/jcsl/krw018.
[107] Tallinn manual 2.0, *supra* note 26 at 398.
[108] Congressional Research Service, *Russian Military Intelligence: Background and Issues for Congress* 4 (Nov. 15, 2021), https://fas.org/sgp/crs/intel/R46616.pdf.
[109] Tallinn manual 2.0, *supra* note 26 at 397.
[110] Congressional Research Service, *supra* note 108 (the true structure of the GRU is not known).
[111] Open Sanctions, *Igor Olegovich Kostyukov* (last accessed Aug. 10, 2024), https://www.opensanctions.org/entities/Q59021350/.
[112] Congressional Research Service, *supra* note 108.
[113] Tallinn manual 2.0, *supra* note 26 at 398.
[114] *Id.* at 396.
[115] *Id.*
[116] *Id.* at 399.

not hold much weight, in light of the hypothesis regarding the existence of a common plan or policy. Nevertheless, should hackers like Sandworm or Fancy Bear be deemed 'most responsible', an additional layer of difficulty must be considered insofar as individuals play different roles in COs, ranging from the design of the malware to executing the payload.[117] Therefore, on an individual level, the members of a hacking Unit may be viewed to hold different degrees of responsibility.

In either case, the requisite *mens rea* is crucial when analysing COs. The RS adopts a fairly restrictive approach to the requirements of "*intent*" and "*knowledge*",[118] the standard for the foreseeability of events which would constitute war crimes being virtual certainty.[119] Academia has underlined that hackers, due to their absence of proximity to the targeted infrastructure, in comparison to traditional troops, may be deprived of the ability to assess the situation in the targeted area, especially in regard to proportionality.[120] On the other hand however, in the case of COs being launched by state actors, it appears difficult that infamously notorious groups, such as Sandworm or Fancy Bear, lacked *mens rea.*[121]

Therefore, the nature of COs poses an additional challenge to determining the identity of those individuals who are the 'most responsible', and their respective responsibility. In the case of the Russo-Ukrainian conflict, a presumption is posited in favour of that superior commanders were most responsible, insofar as a common plan is found. This, however, does not bar the possibility of finding that hackers should be the ones investigated, and ultimately, prosecuted.

[117] Marco Roscini, *supra* note 82 at 257.
[118] Jennifer Trahan, *Criminalization of Cyber-operations Under the Rome Statute*, 19 no. 5 Journal of International Criminal Justice 1133, 1150 (Nov. 8, 2021), https://doi.org/10.1093/jicj/mqab066.
[119] *The Prosecutor v. Thomas Lubanga Dyilo*, ICC-01/04-01/06 A 5, Judgment on the appeal of Mr Thomas Lubanga Dyilo against his conviction, ¶ 447 (Dec. 1, 2014).
[120] Tallinn manual 2.0, *supra* note 26 at 396.
[121] Art.30 RS; *Also see* Tallinn manual 2.0, *supra* note 26 at 392.

II. Are attacks against a nation's energy grid or electrical infrastructure war crimes in accordance with Article 8(2)(b) of the Rome Statute?

Should COs directed against electrical systems give rise to sufficiently grave situations for a case to be admissible, it nevertheless remains to be determined whether the subject-matter jurisdiction of the ICC can be engaged. Specifically, it must first be ascertained whether attacks against electrical systems fall under the specified prohibitions of Art.8 RS and, second, whether COs thus constitute new means of perpetrating, or otherwise contributing to, war crimes, in accordance with Article 25(3) RS.

Given that the Russo-Ukrainian War evidences the particular characteristics of cyber-enabled warfare, that is, kinetic and cybernetic attacks being launched conjunctly against a set target, this analysis will centre on the premise that the COs must thus be considered part of an overall attack. Responsibility would then be engaged in accordance with Art.25(3)(d) for contributing to the commission of war crimes. However this Paper acknowledges that COs, in determined cases, may in and of themselves give rise to sufficiently grave situations. Therefore, if these attacks against electrical systems are deemed unlawful, COs would constitute new means of perpetrating war crimes.

Furthermore, since electrical systems have been the object of military operations since the First World War,[122] there is no straightforward answer under Public International Law. The Russo-Ukrainian conflict represents an occasion to draw a path for the future of international criminal prosecution, by acknowledging evolving changes in warwaging. Particularly, it showcases the practical application of a historical theoretical debate, and is the catalyst for reconsidering existing benchmarks. In this analysis, this Paper aims at highlighting existing gaps, dissent, and considerations for other circumstances, to offer a realistic overview of the case to be made against attacks targeting electrical systems. However, it acknowledges that this exploration only opens the

[122] *E.g.*, James W. Crawford III, *supra* note 1.

gates for reconsidering the *status quo*, therefore it is not a universally definite answer. It may be advanced that the latter may only proceed from the Court defining the applicable legal standards, as a result of the war, which will be explored in Chapter III.

Proceeding, the Russian Federation's repeated and widespread targeting of electrical infrastructure has sparked numerous accusations of war crimes.[123] Research is now centering on demonstrating that the ICC could possess subject-matter jurisdiction, that is, that the operations could fall under the prohibitions set out in Article (8)(2)(b)(i), (ii), (iv), and (xxv) RS.[124] It must be underlined here that Chapter I already determined that these prohibitions encompass their transgressing through kinetic and cybernetic means,[125] because the principles of necessity, proportionality, and distinction, also apply to the use of ICTs by States.[126]

Art.8(2)(b)(i) bars "*intentionally directing attacks against the civilian population*". AP I establishes that "*acts or threats of violence the primary purpose of which is to spread terror among the civilian population*" are specifically prohibited.[127] It has repeatedly been emphasised that these infringements of IHL also constitute war crimes against civilians.[128] The international community has denounced that Russia's attacks against electrical infrastructure appear

[123] *E.g.*, Amnesty International, *supra* note 70; Gregory P. Noone et al., *Are Russian Attacks on Ukraine's Electrical Grid a War Crime?,* Center for Civil Liberties (Aug. 10, 2023), https://ccl.org.ua/en/positions/are-russian-attacks-on-ukraines-electrical-grid-a-war-crime/.
[124] Michael N. Schmitt, *Ukraine symposium – attacking power infrastructure under international humanitarian law*, Liber Institute West Point (Oct. 20, 2022), https://lieber.westpoint.edu/attacking-power-infrastructure-under-international-humanitarian-law/.
[125] International Committee of the Red Cross, *supra* note 27 at 486-7.
[126] U.N. GAOR, *supra* note 34; Tallinn manual 2.0, *supra* note 26 at 420 & 470.
[127] Art.51(2) AP I.
[128] International Committee of the Red Cross, *Practice Relating to Rule 2. Violence Aimed at Spreading Terror among the Civilian Population*, *in* International Humanitarian Law Databases (last accessed Aug. 10, 2024), https://ihl-databases.icrc.org/en/customary-ihl/v2/rule2.

primarily designed to instil terror.[129] Human rights experts,[130] researchers,[131] and industry actors,[132] have all clearly stressed that there appears to be a correlation between an increase in strikes, and the onset of winter, thus labelling the acts as deliberately cruel.[133] Statements by Russian government officials, such as requesting for their demands to be met to "*end all possible suffering of the local population*",[134] and wishing for citizens to "*freeze and rot*",[135] further support this hypothesis. Furthermore for some academics, the intensity and frequency of the strikes, as will be further expounded on below, render the verification of the legitimacy of each target impossible. Consequently, this would demonstrate that Russia's main motivation, at least in some attacks, is to terrorise.[136]

To qualify as a 'terror attack', the victims must "*suffer grave consequences (...) which may include (...) death and/or serious injury*", also encompassing

[129] *E.g.,* Human Rights Watch, *Ukraine: Russian Attacks on Energy Grid Threaten Civilians* (Dec. 6, 2022, 12:01 AM), https://www.hrw.org/news/2022/12/06/ukraine-russian-attacks-energy-grid-threaten-civilians.
[130] *E.g.*, *Id.*
(*See* Yulia Gorbunova, senior Ukraine researcher at Human Rights Watch).
[131] *E.g.*, Ben Tobias, *Is attacking Ukraine's power grid a war crime?*, BBC (Dec. 1, 2022), https://www.bbc.com/news/world-europe-63754808 (Doctor Maria Varaki, King's College War Studies Department).
[132] *E.g.*, Daryna Antoniuk & Alexander Martin, *Life during wartime: Ukraine 'has to be ready for new more powerful and complex' cyberattacks*, The Record (Jan. 11, 2023), https://therecord.media/life-during-wartime-ukraine-has-to-be-ready-for-new-more-powerful-and-complex-cyberattacks.
(DTEK, Ukraine's largest private sector company).
[133] Amanda Macias, *Pentagon says Moscow's deliberate targeting of Ukrainian energy grids is a war crime*, CNBC (Nov. 16, 2023, 5:03 PM), https://www.cnbc.com/2022/11/16/targeting-of-ukrainian-energy-grid-is-a-war-crime-pentagon-says.html.
(*See* Statement by U.S. Defence Secretary, Llyod Austin).
[134] Humanitarian Research Lab at Yale School of Public Health & Ukraine Digital Verification Lab, *Remote Assessment of Bombardment of Ukraine's Power generation and Transmission Infrastructure* 14 (Feb. 29, 2024), https://hub.conflictobservatory.org/portal/sharing/rest/content/items/d4cc5cda5be1443ea1fc1ff52cc89e45/data, (Referring to the Press Secretary of the President of the Russian Federation, Dmitri Peskov).
[135] Francis Scarr, X (Nov. 26 2022, 9:17 AM), https://x.com/francis_scarr/status/1596417788616536064.
(Re-posting critically the televised interview given by Boris Chernyshov, a Deputy Speaker of the State Duma of the Russian Federation. Chernyshov holds in his interview that Ukrainians should "freeze and rot" in their homes.)
[136] *E.g.,* Michael N. Schmitt, *Ukraine Symposium – Further thoughts on Russia's campaign against Ukraine's power infrastructure*, Lieber Institute West Point (Nov. 25, 2022), https://lieber.westpoint.edu/further-thoughts-russias-campaign-against-ukraines-power-infrastructure/.

"*trauma and psychological damage*".[137] It is not required that civilians have actually been terrorised, for it is sufficient that terror was specifically intended.[138] This purpose may be inferred from the nature of the attack,[139] hereby of closest analogy, indiscriminate and widespread shelling.[140] Again tactical similarities in this reference may be found, insofar as Russia has been accused of striking electrical systems regardless of any military advantage, across widespread Ukrainian territory.[141]

However, there are two central issues to this conjecture. First, the primary purpose or *mens rea* of the adversary in targeting electrical systems can only be hypothesised. Whereas some academics, initially reticent to call the strikes 'terror' attacks,[142] modified their analysis after the start of large-scale operations in October 2022,[143] others remain firm in asserting that, although a purpose to terrorise may be identified, it cannot be firmly established as primary, or established at all.[144] Secondly, when comparing the targeting of electrical systems to the international case law on terror attacks, it appears to fall short from the grave attacks previously categorised. For instance, past cases have regarded directly shelling civilians,[145] or rocket attacks against civilians.[146]

In view of that it is unlikely that the ICC would be able to able to proceed on the basis that the operations fall under the prohibition of Art.8(2)(b)(i) RS, focus may be placed on the second accusation that Russia's strikes infringe upon

[137] The Prosecutor v. Radovan Karadžić, Case No. IT-95-5/18-T, Judgment, ¶ 461 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 24, 2016).
[138] The Prosecutor v. Stanislav Galić, Case No. IT-98-29-A, Judgment, ¶ 104 (Int'l Crim. Trib. for the Former Yugoslavia, Nov. 30, 2006).
[139] Eirini Giorgou & Abby Zeith, *When the lights go out: The protection of energy infrastructure in armed conflict*, Humanitarian Law & Policy (Apr. 20, 2023), https://blogs.icrc.org/law-and-policy/2023/04/20/protection-energy-infrastructure-armed-conflict/.
[140] U.N. GAOR 53rd Sess., Item 110(c) G.A. Res.*53/164* at 2 (Feb., 1999).
[141] *E.g.*, Gregory P. Noone et al., *supra* note 123; Michael N. Schmitt, *supra* note 136.
[142] Michael N. Schmitt, *supra* note 124.
[143] Michael N. Schmitt, *supra* note 136.
[144] Charlie Dunlap, *Is attacking the electricity infrastructure used by civilians always a war crime?*, Lawfire (Oct. 27, 2022), https://sites.duke.edu/lawfire/2022/10/27/is-attacking-the-electricity-infrastructure-used-by-civilians-always-a-war-crime/.
[145] *The Prosecutor v. Dragomir Milošević*, Case No. IT-98-29/1-T, Judgment, ¶ 912 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 12, 2007).
[146] *The Prosecutor v. Milan Martić*, Case No. IT-95-11, Decision, ¶ 31 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 8, 1996).

the prohibition of attacking "*civilian objects*" within the meaning of Art.8(2)(b)(ii).

Not defined in the RS, civilian objects are however generally understood as those objects normally used by, or dedicated to, civilians and civilian purposes.[147] Energy provision systems are a prime example of infrastructure now deemed critical to civilians.[148] Furthermore, the categorisation of objects as civilian is made in the negative, that is, all objects which are not military objectives (hereinafter, MOs).[149] According to State practice, the latter refers to whether, to begin with, by its nature, location, purpose, or use, the electrical system makes an effective contribution to military action and, then, whether its total or partial destruction or neutralisation offers a definite military advantage.[150]

Academia has underlined that those components or parts of electrical systems which enable the provision of services to civilians benefit from a presumption of civilian status. This means that, in case of doubt as to whether a piece of infrastructure is being used to make an effective contribution to military action, the object must be presumed to be civilian.[151] Following from the above hypothesis that the Russian Federation has not been able to, or has not carried out, the required due diligence to differentiate between electrical systems which qualify as MOs, and civilian objects, the current state of evidence does support a presumption in favour of that, at least some of the targeted infrastructure, were civilian objects.[152]

Indeed on the one hand, those planning and deciding upon attacks against electrical systems must do so on the basis of robust, multidisciplinary intelligence assessments, which comprehensively map the effects on civilians and the impact on the adversary's military capabilities.[153] On the other hand, Russia

[147] Eirini Giorgou & Abby Zeith, *supra* note 139.
[148] *See generally, e.g.,* Human Rights Watch, *supra* note 129.
[149] Art.52(1) AP I.
[150] Art.52(2) AP I.
[151] Art.52(3) AP I.
[152] Michael N. Schmitt, *supra* note 136.
[153] Thomas E. Griffith Jr., *Strategic Attack of National Electrical Systems*, Air University Press 45 (Oct. 1994),

has been striking the Ukrainian electricity grid and infrastructure on a widespread scale, geospatially across the country, and temporally since the beginning of the invasion. A study, published during the writing of this Paper in late February 2024, highlights that the aforementioned scale in attack is "*consistent with a widespread and systematic effort to cripple vital power generation*" for civilians.[154] It uncovers that the 223 attacks against electrical systems which could be identified spun across 23 out of 24 oblasts.[155] It is important to note as well that, out of the 216 they could spatially locate, 128 occurred in oblasts that did not have a frontline running through them at the time.[156] Again, to the day of the writing of this Chapter, Russia is still strongly striking against the power grid.[157] Having highlighted above that academics are highly sceptical that Russia conducted the due diligence of status verification with each target,[158] on this ground they conclude that the sweeping classification of the entire electrical grid of a country as a MO must violate the norms of IHL. Notably, it infringes upon the principle of distinction by carrying out indiscriminate attacks.[159]

Nevertheless, doubts arise regarding whether the conduct identified falls under the scope of this prohibition. Electrical systems are typically categorised as "*dual-use*" or "*dual-purpose*" objects, meaning that the grid or infrastructure is being used by, or can equally serve the purposes of, civilians and the military, in accordance with the first prong of the definition of MO.[160] Electrical systems

https://media.defense.gov/2017/Dec/29/2001861964/-1/-1/0/T_GRIFFITH_STRATEGIC_ATTACK.PDF.

[154] Humanitarian Research Lab at Yale School of Public Health & Ukraine Digital Verification Lab, *supra* note 134 at 14.

[155] *Id.* at 8.

[156] *Id.* at 4.

[157] Max Hunder & Tom Balmforth, *Russia pounds Ukrainian power facilities, Zelenskiy seeks air defences, 'political will',* Reuters (Mar. 23, 2024, 12:35 AM), https://www.reuters.com/world/europe/ukraine-says-russian-strike-hit-ukraines-largest-dam-during-mass-strike-energy-2024-03-22/ (On March 22nd, 2024, the Russian Federation launched the largest airstrike on energy infrastructure to date in the Russo-Ukrainian War).

[158] Ben Tobias, *supra* note 131 (BBC interviewing Michael N. Schmitt).

[159] *E.g.*, Michael N. Schmitt, *supra* note 136; Eirini Giorgou & Abby Zeith, *supra* note 139.

[160] *E.g.*, Human Rights Watch, *supra* note 129; U.S. Department of Defense, *Law of War Manual* § 5.6.1.2 (July 31, 2023), [hereinafter, DoD Manual].

have indeed numerous times been deemed MOs,[161] either because they power military installations, equipment, or activities (the "*use*" criterion), or because they may be used to do so in the future (the "*purpose*" criterion).[162] In either case, it must make an "*effective contribution to military action*," that is, there must be a proximate nexus between the infrastructure and the fighting.[163] Regarding electrical systems, this requirement typically relates to use or purpose for tactical or operational activities, such as a power station providing electricity to barracks or communication systems, or even strategic uses or purposes, such as diminishing air-defence capabilities by denying radars' use.[164] According to the prevailing military doctrine, modern warfighting is dependent on electricity for effective action,[165] and Ukraine's defences are in effect reliant on the commercial power grid to fend off Russia's attacks.[166] If the Russian Federation can demonstrate that each of the targeted sites was being used by the Ukrainian military for, or could serve the purpose of, effective defensive or offensive action, the first step for categorisation as MO would be satisfied.

Regarding the second prong of the definition, targeting the electrical system must additionally offer a "*definite military advantage*" for the attacker, that is, beyond potential or indeterminate.[167] Although Russian officials claim that they attack electrical infrastructure in furtherance of their military objectives,[168] an informed analysis on whether the adversary obtained such an

[161] International Committee of the Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* 632 (1987); DoD Manual, *supra* note 160 at § 5.6.8.5.
[162] Michael N. Schmitt *supra* note 124; International Committee of the Red Cross, *supra* note 161 at 635.
[163] ICRC Delegation to the EU, NATO and the Kingdom of Belgium, 18th Bruges Colloquium, *The Additional Protocols at 40: Achievements and Challenges* 140 (Luis B. García et al. eds., 2017), https://www.coleurope.eu/sites/default/files/uploads/page/collegium_48_webversie.pdf.
[164] Eirini Giorgou & Abby Zeith, *supra* note 139.
[165] Francesa Capone, *The wave of Russian attacks on Ukraine's power infrastructure: An opportunity to infuse meaningfulness into the notion of "dual-use objects"*, 8 no. 2 European Forum 741, 746 (Nov. 2023), doi: 10.15166/2499-8249/684.
[166] Charlie Dunlap, *supra* note 144 (Citing Dunlap, "For example, experts say the Starlink, a privately-owned system that provides internet service—and is obviously dependent upon electrical power—has "become an essential tool for the Ukrainian military to coordinate across thousands of kilometres of combat theatre.").
[167] International Committee of the Red Cross, *supra* note 161 at 635.
[168] U.S. Dep't of State, *FPC Briefing – Russian Attacks Targeting Ukraine's Energy Infrastructure* (Mar. 4, 2024, 11:00 AM), https://www.state.gov/briefings-foreign-press-centers/russian-attacks-targeting-ukraine-energy-in

advantage is difficult to construct. This matter will be further explored below. It is however possible that this second step is fulfilled, especially since the threshold is lower than that which is applied in the proportionality test ["*concrete and direct military advantage*"].[169] Consequently, the system would no longer be classified as civilian but military,[170] and military action against these objects would not be precluded. Instead, it would be subject to the test of proportionality.

Reiterating, in view of the temporal and geographical spread of the attacks, it appears unlikely that Russia each time legitimately targeted MOs exclusively, falling under the scope of the prohibition of Art.8(2)(b)(ii) RS. However, even if some of the attacks fell under the scope of this prohibition because the infrastructure qualified as a civilian object exclusively, given that electrical systems are most often dual-use, the targets may also in other instances have been MOs. The Russian Federation's attacks may thus additionally fall under this prohibition. Namely, Art.8(2)(b)(iv) encompasses the RS's proportionality analysis, prohibiting "*intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects* (...) *which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated*".

To begin with, based on publicly available information, pinpointing the advantage which Russia sought to obtain from the destruction of electrical systems is not straightforward. Moreover, even if such data was available, contrasting stances emerge regarding the applicable benchmark. According to the ICRC, "*concrete and direct*" refers to a substantial and relatively close advantage.[171] Meanwhile, the U.S. Department of Defense's Manual (hereinafter, DoD Manual) assesses "*the full context of the war strategy*", a much broader

frastructure, (Interview with Nathaniel A. Raymond, Executive Director and Researcher at the Yale Humanitarian Research Lab, and with Caitlin Howarth, Director of Operations for the Conflict Observatory Team of the Yale Humanitarian Research Lab).

[169] Francesa Capone, *supra* note 165 at 745.

[170] International Committee of the Red Cross, *Rule 8. Definition of Military Objectives*, *in* International Humanitarian Law Databases (last accessed Aug. 10, 2024), https://ihl-databases.icrc.org/en/customary-ihl/v1/rule8; DoD Manual, *supra* note 160 at § 5.6.1.2.

[171] International Committee of the Red Cross, *supra* note 161 at 684.

scope.[172] A further example is that the Study Group on the Conduct of Hostilities in the 21st Century agreed that the notion of 'concrete and direct' does not include advantages that are only moral in nature,[173] whereas the DoD Manual holds that diminishing morale constitutes an advantage.[174] In any and all cases, the Kremlin has sought to justify the attacks using the language of AP I,[175] for instance stating that the targeted infrastructures "*support the functioning of the (...) military industrial complex*".[176]

Traditional military orthodoxy supports this contention.[177] Drawing from known facts, in relation to past conflicts such as NATO's Campaign in Kosovo, or the War in Iraq,[178] targeting electrical systems was concluded to wield extensive military advantages. For instance, it has long been accepted that the nullification of electricity can provide a short-term or tactical military advantage with respect to the degradation of air-defence systems.[179] The latter are crucial in the case of Ukraine.[180] However it must be nuanced that, in regards to these very same conflicts, whereas some experts praised the achievement of "*remarkably little collateral damage*",[181] contrasting academia emerged to underline the numerous civilian deaths which result from the systematic elimination of electrical power in the aftermath of the war. Thereby, they question whether the usefulness of the tactic is not based on unsubstantiated presumptions.[182]

[172] DoD Manual, *supra* note 160 at § 5.6.7.3.
[173] International Law Association Study Group on the Conduct of Hostilities in the 21st century, *The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare*, 93 International Law Studies U.S. Naval War College 322, 363 (2017), ISSN 2375-2831
[174] DoD Manual, *supra* note 160 at § 5.6.7.3.
[175] Humanitarian Research Lab at Yale School of Public Health & Ukraine Digital Verification Lab, *supra* note 134 at 13.
[176] *Id.* (Statement by the Russian Federation's Ministry of Defense).
[177] James W. Crawford III, *supra* note 1 at 102; Thomas E. Griffith Jr. *supra* note 153 at 15.
[178] James W. Crawford III, *supra* note 1 at 109.
[179] James W. Crawford III, *supra* note 1 at 113.
[180] Olivia Yanchik, *Ukraine needs enhanced air defences as Russia expands missile arsenal*, Atlantic Council (Mar. 2, 2022), https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-needs-enhanced-air-defenses-as-russia-expands-missile-arsenal/.
[181] Eliot A. Cohen et al., *Gulf War Air Power Survey. Volume II. Operations Effect and Effectiveness* Part II at 343 (Jan. 1, 1993), https://apps.dtic.mil/sti/citations/ADA279742.
[182] James W. Crawford III, *supra* note 1 at 102 (Extends to other conflicts, including World War II, Korea and Vietnam).

Electrical systems indeed represent a point of contention amongst academia and practitioners insofar as the scope of the notion of 'military advantage' is concerned, both for qualification as MO, and for the application of the proportionality test. This debate has not been settled and, due to the extensive nature of the dispute, it will not be further explored for the purposes of this Chapter. Nevertheless, the outcome of this analysis will be predominantly influenced by the ICRC's position, which affords heightened protections to civilians due to its advocacy for a narrow definition of MO and, as will be explored below, for the inclusion of reverberating effects in the assessment of harm. This interpretational decision is based on the interaction between the ICC's interpretations and the ICRC's position, which are more closely aligned in comparison to the American military standpoint.[183] Regardless, even when drawing from past conflicts, not much at this stage can be determined regarding whether the Russian attacks on the Ukrainian electricity grid truly yielded them a concrete and direct military advantage for the purposes of Art.8(2)(b)(iv).

In contrast, prominent military,[184] political,[185] and academic figures,[186] have characterised the Russian attacks as a deliberate targeting of civilian power generation facilities, causing excessive collateral damage and unnecessary suffering. The key to this assessment, however, is the extent of collateral damage which must be accounted for in the proportionality test,[187] or else, which repercussions on civilians were foreseeable byproducts of the attack.[188] Regarding electrical systems, extensive research has also already been carried

[183] *See generally* International Committee of the Red Cross, *ICRC and ICC: Two separate but complementary approaches to ensuring respect for international humanitarian law*, (Mar. 3, 2009), https://www.icrc.org/en/article/icrc-icc-international-humanitarian-law. (Interviewing Anne-Marie La Rosa, legal adviser and focal point for the ICRC on issues related to international criminal justice).
[184] Interview Transcript with Secretary of Defense Lloyd J. Austin III, and Army General Mark A. Milley, Chairman, Joint Chiefs of Staff, *Press Briefing Following Ukrainian Defense Contract Group Meeting*, U.S. Department of Defense (Nov. 16, 2022), https://www.defense.gov/News/Transcripts/Transcript/Article/3220910/secretary-of-defense-lloyd-j-austin-iii-and-army-general-mark-a-milley-chairman/.
[185] U.N. SCOR, 9256th mtg., U.N. Doc. S/PV.9256 (Feb. 8, 2023, 10:00 AM) (Briefing by Izumi Nakamitsu, Under-Secretary General and High Representative for Disarmament Affairs).
[186] Human Rights Watch, *supra* note 129 (Referring to Yulia Gorbunova, senior Ukraine Researcher at Human Rights Watch).
[187] Michael N. Schmitt, *supra* note 124.
[188] Michael N. Schmitt, *supra* note 124.

out,[189] albeit without reaching an agreement on how to best factor the civilian element in the calculus.[190] The discussion spans out very similarly to the academic views explored in Chapter I, regarding the scope of the consequences which must be accounted for, that is, direct and/or indirect effects.[191] For instance, although the DoD Manual only accounts for "*immediate or direct harms*", it expands its construction to that "*the destruction of a power plant would be expected to cause loss of life (...) very soon after the attack due to the loss of power at a connected hospital*".[192] The ICRC goes a step further, prescribing that parties to an armed conflict are obliged to take into account the reasonably foreseeable reverberating effects of an attack.[193] The latter has gained the most support amongst academia.[194] Yet, doubts also emerge regarding the scope and nature of this duty, including the necessary degree of causation, or when reverberating effects should be deemed too remote to be considered a consequence of the attack.[195]

In the case of Ukraine, the strikes have not only led to direct civilian deaths in the vicinities of the target,[196] but over the course of the war thousands of towns and cities have faced rolling blackouts,[197] depriving civilians of heating in average territorial temperatures of -2 to -4.8 degrees Celsius, with some regions regularly reaching -21.6.[198] Regional Director of the World Health Organization for Europe, Dr. Hans Henri Kluge, emphasised that "*cold weather can kill*".[199] Civilian testimonies and reports further depict the wide range of

[189] *See generally, e.g*, Michael N. Schmitt, *The Principle of Discrimination in 21st century warfare,* 2 Human Rights and Development Law Journal 143, 168 (1999), http://dx.doi.org/10.2139/ssrn.1600631.
[190] Francesa Capone, *supra* note 165 at 752.
[191] Michael N. Schmitt, *supra* note 124.
[192] DoD Manual, *supra* note 160 at § 5.12.1.3.
[193] Isabel Robinson & Ellen Nohle, *Proportionality and precautions in attack: The reverberating effects of using explosive weapons in populated areas,* 98 no. 901 International Review of the Red Cross 107, 112 (Apr., 2016), https://doi.org/10.1017/S1816383116000552.
[194] *Id.* at 112 n.30.
[195] *Id.* at 117.
[196] Hugo Bachega & Yaroslav Lukov, *supra* note 71.
[197] *E.g.*, Hugo Bachega & Yaroslav Lukov, *supra* note 71.
[198] International Rescue Committee, *What Ukrainians need to survive winter* (Nov. 8, 2023), https://www.rescue.org/eu/article/what-ukrainians-need-survive-winter.
[199] World Health Organization [WHO], *Statement – Winter in Ukraine: people's health cannot be held hostage* (Nov. 21, 2022), https://www.who.int/europe/news/item/21-11-2022-statement---winter-in-ukraine--people-s-health

difficulties which are associated with the prolonged lack of secure access to electricity: a grandmother melting snow for water,[200] surgeons operating with flashlights,[201] cancer patients dependent on oxygen trying to charge their concentrator,[202] or a mother trying to cook for her children as food continues to perish,[203] are a few select stories. Widespread reverberating impacts on the provision of basic necessities such as food, water, and medical assistance, particularly affecting vulnerable groups such as children, the elderly, and the sick, may thus account for the purposes of the proportionality assessment.

Although it is highly plausible that the operations also fell under the prohibition of Art.8(2)(b)(iv), if the ICRC's stance is adopted, this conclusion is not definitive. A comprehensive review will depend on the obtention of evidence regarding the advantage Russia sought to obtain, and weighing the latter against a qualitative and quantitative analysis of the civilian impact. However, based on the information gathered regarding the significant effects of electricity deprivation on civilians' livelihood, it must lastly be explored whether Russia's attacks could fall under the scope of the prohibition encompassed in Art.8(2)(b)(xxv).

The latter refers to "*intentionally using starvation of civilians as a method of warfare by depriving them of objects indispensable to their survival*". According to Art.54(2) AP I, the mentioned objects include foodstuffs, agricultural areas for food production, crops, livestock, drinking water installations and supplies, and irrigation works. In such a case, even if the objects directly support military

-cannot-be-held-hostage, (Statement by Hans Henri P. Kluge, WHO Regional Director for Europe).

[200] Reliefweb, *Heating bricks and melting ice: Creative ways Ukraine families are surviving this winter* (Jan. 26, 2023), https://reliefweb.int/report/ukraine/heating-bricks-and-melting-ice-creative-ways-ukraine-families-are-surviving-winter.

[201] Yuras Karmanau et al., *Surgeons work by flashlight as Ukraine power grid battered*, AP News (Nov. 28, 2022, 4:40 PM), https://apnews.com/article/russia-ukraine-health-europe-covid-duda-c84f2292b25ce67724adf8ade78f2f45.

[202] Human Rights Watch, *supra* note 129.

[203] Amnesty International, *Ukraine: Devastating power cuts undermining civilian life as Christmas approaches* (Dec. 21, 2022), https://www.amnesty.org/en/latest/news/2022/12/ukraine-devastating-power-cuts-undermining-civilian-life-as-christmas-approaches/.

action, targeting is nevertheless prohibited if it is expected to leave the civilian population with such inadequate quantities of food or water as to cause its starvation.[204]

Accordingly, although electrical systems are not specifically mentioned, Russian attacks have been denounced to cause a peril of starvation.[205] More precisely, basic human survival is thought to be severely impacted,[206] as the power outages continuously result in entire regions, and millions of civilians, having impaired access to drinking water.[207] The aforementioned list of objects being nonexhaustive,[208] the disruption of electrical infrastructure may indeed be the necessary corollary to this prohibition. Military academia and international organisations have recognised that energy is now indispensable to the functioning of the objects that are necessary to the survival of civilians.[209] To this end, the ICRC has extensively stressed that damage to components of an electricity network may affect water purification, storage, and distribution systems.[210] Again, in lack of comprehensive data-based reports on the matter from Ukraine, past conflicts offer an illustration. In Iraq, the strikes impeded the refrigeration of vaccines, limited the capability to purify water, and dispose of raw sewage, thereby increasing the number of victims of waterborne diseases,

[204] Art.54(3)(b) AP I.
[205] *E.g.,* Human Rights Council, 52nd Sess. Item 4, *Report of the Independent International Commission of Inquiry on Ukraine* 7*,* U.N. Doc. A/HRC/52/62; Michael N. Schmitt, *supra* note 136; Human Rights Watch, *supra* note 129.
[206] Sec'y of Def. Lloyd J. Austin III & ARMY Gen. Mark. A. Milley, *Transcript: Secretary of Defense Lloyd J. Austin III and Army General Mark A. Milley, Chairman, Joint Chiefs of Staff, Hold a Press Briefing Following Ukrainian Defense Contact Group Meeting*, US Dep't of Def. (Nov. 16, 2022), https://www.defense.gov/News/Transcripts/Transcript/Article/3220910/secretary-of-defense-lloyd-j-austin-iii-and-army-general-mark-a-milley-chairman/.
[207] Michael N. Schmitt, *supra* note 136; Human Rights Council, *supra* note 205.
[208] International Committee of the Red Cross, *supra* note 161 at 655.
[209] *E.g.*, Michael N. Schmitt, *supra* note 136; Security Council Report, *Arria-formula Meeting: Protection of Water-related Essential Services and Infrastructure During Armed Conflicts* (Mar. 21, 2023), https://www.securitycouncilreport.org/whatsinblue/2023/03/arria-formula-meeting-protection-of-water-related-essential-services-and-infrastructure-during-armed-conflict.php; Henry Shue & David Wippman, *Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions*, 35 no. 3 art. 7 Cornell International Law Journal 559, 573 (2002), http://scholarship.law.cornell.edu/cilj/vol35/iss3/7.
[210] Isabel Robinson & Ellen Nohle, *supra* note 193 at 132.

and decreasing crop yields due to reduced irrigation capabilities.[211] According to the ICRC, these factors also account for the purposes of the proportionality test, especially insofar as a reasonable military commander is expected to foresee that destroying electricity facilities will cut off the civilian fresh water supply.[212] Moreover, if this very same commander knows that water distribution or treatment is already operating at a low capacity, he should know that the effects on civilians caused by further damage to the plant will be more significant than if the plant was fully functioning.[213] In Ukraine, already before the war, 40% of its water supply networks were in a critical condition.[214] Thus, Russian strikes have significantly further hampered the ability to maintain distribution.[215]

Nevertheless, although this analysis reinforces a presumption in favour of the Russian attacks falling under the prohibition of Art.8(2)(b)(iv), regarding the conduct being encompassed by Art.8(2)(b)(xxv), it appears unlikely. As was already posited in the commentary under Art.8(2)(b)(i), demonstrating the intention to starve civilians is perhaps an insurmountable obstacle, because the impact of the attacks on basic necessities may be considered a remote consequence for the purpose of proving *mens rea.*

III. Partial Conclusion

Attacks against a nation's energy grid can be considered war crimes, since they may give rise to sufficiently grave situations to cross the admissibility threshold, and may fall under the scope of the specified provisions of Art. 8 RS.

---

[211] James W. Crawford III, *supra* note 1 at 110.
[212] Isabel Robinson & Ellen Nohle, *supra* note 193 at 121.
[213] *Id.* at 125.
[214] World Bank, *Ukraine Water Supply and Sanitation Policy: Toward Improved, Inclusive, and Sustainable Water Supply and Sanitation Services* 3, (last accessed Aug. 11, 2024), https://documents1.worldbank.org/curated/en/844681624034932176/pdf/Ukraine-Water-Supply-and-Sanitation-Policy-Note-Toward-Improved-Inclusive-and-Sustainable-Water-Supply-and-Sanitation-Services.pdf.
[215] Angus Soderberg, *Navigating Russia's Attacks on Water and Energy in Ukraine*, American Security Project (Mar. 10, 2023), https://www.americansecurityproject.org/navigating-russias-attacks-on-water-and-energy-in-ukraine/.

This Paper however has determined that numerous challenges arise in the way of deeming this conclusion definitive.

First, whether COs targeting a nation's energy grid give rise to sufficiently grave situations depends on the tactics employed in attack. Although a standalone attack, cybernetic or kinetic, may not reach the threshold, when there is a conjunct deployment of COs and conventional weapons, as in Ukraine, or COs alone, which rise to the sufficient level of scale, and thus impact in attack, the test may be satisfied. This is in any case dependent on reverberating effects accounting for this test. Furthermore, demonstrating that those who will likely be the object of investigation are the 'most responsible' remains the subject of contention. COs' particular technical characteristics confront mixed theories on the respective knowledge which hackers possess, as opposed to superior military commanders, regarding the attack and the battlefield.

Second, several obstacles still stand in the way of demonstrating that such attacks fall under the scope of specified prohibitions. It may however be generally drawn that widespread and indiscriminate targeting of a nation's electrical grid and infrastructure can be encompassed by provisions of Art.8(2)(b)(ii) and (iv). The latter observation is weapons-neutral since, although the Russo-Ukrainian War exemplified a case of cyber-enabled warfare, insofar as COs alone could impede electricity production or distribution in the same manner as kinetic strikes, they thereby also attack objects and, in effect, can disproportionately impact civilians. However, the difficulties highlighted in regards to the assessment criteria which should apply to targeting electrical systems, including by means of COs, underpinned obstacles which have not been provided for in current texts or interpretations, bringing us to Chapter III.

CHAPTER III. The ICC in the context of the Russo-Ukrainian War: role and challenges ahead in facing cyber operations against electrical infrastructure

The Russo-Ukrainian War has shaped the Western perception of armed conflicts and IHL more than any other since the Second World War.[216] Notably, it has uncovered that even when a case is sufficiently grave to be admissible before the ICC, and even where the specified conduct falls under the scope of the prohibitions of Art. 8 RS as a war crime, gaps in existing texts and interpretations need to be filled in order for the Court to engage a case. First, academics disagree on whether the Rome Statute necessitates amendment to afford the Court jurisdiction over cyber-enabled crimes. Second, academia has emerged to suggest that the Court needs to clarify the applicable benchmarks to assessing the legality of targeting electrical systems. This Chapter will thus establish that, subject to that the CO can be technically attributed to a specified hacker or team, and the latter's connection to a Party can be identified, the prohibition of analogy represents a challenge to encompassing cyber-enabled crimes. Therefore the ICC will need to pronounce its stance on the appropriateness of the current writing of the RS. Furthermore this Chapter will uncover that, because electrical systems now power infrastructure critical to civilian survival, the Court will need to take this change into account in what is now a necessary specification of the applicable assessment. The ICC will have to address this latter point in its jurisprudence.

I. The challenge before the ICC and the Rome Statute to encompass cyber-enabled crimes

To delineate the ability of the Court to investigate, and prosecute, COs against electrical systems which fall under a prohibition of Art. 8 RS, it still

[216] Marco Sassòli, *New Challenges and old problems for international humanitarian law,* Lieber Institute West Point (Apr. 3, 2024), https://lieber.westpoint.edu/new-challenges-old-problems-international-humanitarian-law/.

remains to be determined whether the RS, as it is currently written, affords the Court jurisdiction over the crime, that is, cyber-enabled crimes. Particularly, it must be ascertained whether those individuals 'most responsible' for the COs launched against Ukraine's electrical systems could be the object of a prosecutorial process.

This question will be of notable importance in the coming months. Indeed last October 2023, the ICC's lead prosecutor Karim Khan announced that The Hague would for the first time inquire into, and prosecute, hacking crimes which violate international law.[217] Then, on January 22nd, 2024, the Court hosted a conference on addressing cyber-enabled crimes through the RS, although the results of this meeting are yet unknown.[218]

To begin with, Art.8 RS comes into play whenever there is an international armed conflict.[219] Therefore, there must be employment of armed force, and that force must be attributable to one of the parties to the conflict.[220] Regarding the first criterion, although acknowledging that in other cases fulfilment may be complex when in regards to COs, such a question was not the object of this investigation. This Paper having centred on an already active battlefield, the requirement is fulfilled because, where a cyber attack is conducted as part of an ongoing, conventional armed conflict, the armed force threshold is satisfied.[221] On the second prong, the discussion may also be of interest in other circumstances. Notably, whereas in the case of a kinetic strike it may be clear that a particular Party is responsible for it, COs can pose a challenge to technical attribution as the identity of perpetrators is more easily

[217] Yola Verbruggen, *Cybercrimes under consideration by the ICC,* International Bar Association (Oct. 13, 2023), https://www.ibanet.org/cybercrimes-under-consideration-by-the-ICC.
[218] Statement by Karim A. A. Khan on conference addressing cyber-enabled crimes through the Rome Statute System, International Criminal Court (Jan. 22, 2024), https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through.
[219] Art.8(2)(b) RS.
[220] Kai Ambos, *supra* note 48.
[221] *Id.*

shielded in cyberspace.[222] However, the COs of interest to this study have forensically been attributed to Sandworm and Fancy Bear.[223]

Even if the CO can be attributed to a particular hacker or team, a further challenge arises in comparison to the traditional course of analysis. In effect, for said force to be attributable to a Party, an additional step is necessary, which is linking the hacker or team to a State. Again, this is of noteworthy importance in regards to COs, as States may resort to "hackers-for-hire" or "proxies". Yet, in the case of Sandworm or Fancy Bear, they are recognised units of the GRU. Thereby, this Paper further acknowledges that the particularities of cyberspace may warrant further investigation in this regard in other circumstances, and may represent an obstacle for the Rome Statute to encompass cyber-enabled crimes in practical terms.

Proceeding however with the usual course of analysis, although neither Russia nor Ukraine are parties to the RS, the ICC may exercise jurisdiction if a State has accepted it with respect to the crime in question, by means of a declaration.[224] Ukraine exercised this prerogative, to begin with, on April 17th, 2014, when it accepted the ICC's jurisdiction with respect to alleged crimes committed by the Russian Federation from November 21st, 2013 to February 22nd, 2014.[225] Then again, Ukraine extended its acceptance of the ICC's jurisdiction on September 8th, 2015, when it recognized the Court's jurisdiction for an indefinite duration over all crimes against humanity and war crimes perpetrated by the Russian Federation on or after February 20th, 2014.[226]

---

[222] Amply studied and debated, including by *e.g.*, the United Nations Office for Disarmament Affairs (*see generally,* Anastasiya Kazakova et al., *'Unpacking' technical attribution and challenges for ensuring stability in cyberspace. Submission to 2021–2025 UN Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies* (May, 2022), https://documents.unoda.org/wp-content/uploads/2022/05/Unpacking-technical-attribution-and-challenges-for-ensuring-stability-in-cyberspace_Submission-to-the-UN-OEWG.pdf).

[223] CyberPeace Institute, *supra* note 40.

[224] Art.12(3) RS.

[225] International Criminal Court, *Press Release. Ukraine accepts ICC jurisdiction over alleged crimes committed between 21 November 2023 and 22 February 2014,* ICC-CPI-20140417-PR997 (Apr. 17, 2024), https://www.icc-cpi.int/news/ukraine-accepts-icc-jurisdiction-over-alleged-crimes-committed-between-21-november-2013-and-22.

[226] International Criminal Court, *Press Release. Ukraine accepts ICC jurisdiction over alleged crimes committed since 20 February 2014,* ICC-CPI-20150908-PR1146 (Sept. 8, 2015),

However, the COs in return may fall under the jurisdiction of the Court either because they constitute new means to commit a crime over which the ICC has jurisdiction under its Statute, or because they aid, abet, or otherwise assist or contribute to the commission of such a crime.[227] Should COs be considered new crimes, and not new means of committing or contributing to war crimes, their investigation and prosecution would be impossible, for it would contravene the *nullum crimen sine lege* principle in accordance with Art.22(1) RS. This appears unlikely. Meanwhile the impermissibility of analogy, contained in Art.22(2), does pose a considerable issue insofar as it prescribes that "*the definition of a crime shall be strictly construed and shall not be extended by analogy. In case of ambiguity, the definition shall be interpreted in favour of the person being investigated, prosecuted or convicted*". Given that COs are not addressed by the RS, nor IHL,[228] this prohibition is of concern.

The ICC will therefore need to consider whether the RS needs amendment to provide for this gap in the text.[229] Particularly, it may require from the Court to 'fit' COs into the Statute's existing structure for "*directing attacks [against the civilian population, civilian objects etcetera]*".[230] The challenge of aligning COs as "*attacks*" has been explored in Chapter I, however dissenting academia has specifically emerged on the appropriateness of the RS to encompass COs. On the one hand, some academics advocate that the RS can be directly applied to COs, but only to a limited subset of them, that is, destructive COs.[231] On the other hand, some academics posit that the RS does not need to be amended to encompass COs, whether they are destructive or disruptive, if sufficient reverberating damages ensue.[232]

---

https://www.icc-cpi.int/news/ukraine-accepts-icc-jurisdiction-over-alleged-crimes-committed-20-february-2014.

[227] Art.25(3) RS.

[228] Tallinn manual 2.0, *supra* note 26 at 375.

[229] As remains evident from the International Criminal Court [ICC] Forum "Invited Experts on the Cyberwarfare Question" (*See generally supra* note 38), and the January 2024 Conference abovementioned, the question has already been posed by the ICC.

[230] Jennifer Trahan, *supra* note 118 at 1152.

[231] *See generally,* Jennifer Trahan, *supra* note 118.

[232] *See generally*, Marco Roscini, *Cyber Operations Can Constitute War Crimes Under the ICC Jurisdiction Without Need to Amend the Rome Statute*, *in* Cyber Operations and Cyberwarfare Question *in* ICCForum (Mar. 7, 2022), https://iccforum.com/cyberwar.

Academia has generally been in favour of viewing Treaties as living documents, "*to be interpreted in the context of the time in which they are being applied, and not as they would have been interpreted at the time of their drafting*".[233] Regarding the RS specifically, it has already been posited that "*the world today is very different than that which existed when the Rome Statute was drafted and that, to remain effective, the Court must recognize certain conduct that was unforeseen in 1998*". Thereby, where the wording of the Statute can tolerate a proposed meaning, the principle of *nullum crimen sine lege* is not necessarily offended by the ascribing of such meaning, COs, to the provision.[234]

Concludingly, the ICC is now tasked with delineating the future of prosecution in the face of modern warfare. It will specifically need to clarify whether the Rome Statute needs amendment for the ICC to have jurisdiction over cyber-enabled crimes, and thereby successfully prosecute individuals responsible for COs which can qualify as war crimes.

II. The role of the ICC in defining the legality of targeting electrical systems in twenty-first century warfare

Even if the Rome Statute were able to encompass the prosecution of cyber-enabled crimes, the Russo-Ukrainian War has also uncovered further gaps in existing interpretations by reigniting the debate on the legality of attacking a nation's power grid and electrical infrastructure. Particularly, the civilian impact of the invasion has called into question the status of IHL, sparking diverging commentaries such as that the "*Geneva Conventions are still too generic*",[235] or that reinvention is necessary, although "*less with the principles [themselves], and*

[233] Beth Van Schaack & Ronald C. Slye, *International Criminal Law: Essentials* 92 (Nov. 14, 2008), ISBN-13 978-0735565531.
[234] Leena Grover, *Interpreting crimes in the Rome Statute of the International Criminal Court* 184 (Nov., 2014), https://doi.org/10.1017/CBO9781107705586.
[235] Mircea Geoană, North Atlantic Treaty Organisation [NATO] Deputy Secretary General, Conference at the Instituto de Empresa of Madrid [IE University], *NATO in the New Era of Strategic & Industrial Transformation* (Feb. 29, 2024).

more with the sanction, because right now we are failing to sanction those who violate rules".[236]

The debate on the applicable benchmarks and theories will need to be considered by the Court, for it to provide a unified interpretation in its jurisprudence. This will in return allow attacks targeting electrical infrastructure to be encompassed by the scope of the prohibitions. Without a fixed crux of analysis, their encompassment is not definite. In this, the Court will further need to address concerns that the status of electrical systems needs to be revised to account for their emerging interconnection with infrastructure that is essential to civilian survival and,[237] in this exercise, various interpretive challenges to defining the applicable standards arise.

First, the ICC may wish to refine, or redefine, the definition of MO, insofar as academics have criticised the repeated, automatic classification of electrical systems as MOs.[238] The argument in favour of a narrower definition of MOs finds support in the 1956 ICRC Draft Rules for the Limitations of Dangers incurred by the Civilian Population in Times of War. The latter refers to electrical systems as "*industries of fundamental importance for the conduct of war*" when the infrastructure is "*mainly for national defence*".[239] A higher threshold for qualification as MO would in return facilitate encompassing attacks against electrical infrastructure under the umbrella of Art.8(2)(b)(ii)'s prohibition. Currently, it would also strengthen the case against Russia that, in view of the geographical and temporal spread of the attacks, Russia has not verified the legitimacy of each target.[240]

Alternatively, the ICC can consider the application of a more stringent proportionality regime. The ICRC's position, which broadly encompasses the

[236] Agnès Callamard, Secretary General of Amnesty International, Conference at IE University, *Human Rights advocacy in the XXIst century* (Mar. 13, 2024).
[237] *See generally*, most recently International Committee of the Red Cross, *Ukraine: Thousands of families near the frontline receive heating materials to protect against harsh winter conditions* (Jan. 22, 2024), https://www.icrc.org/en/document/ukraine-thousands-families-near-frontline-receive-heating-materials-protect-against-harsh-winter-conditions.
[238] Francesa Capone, *supra* note 165 at 745-51.
[239] International Committee of the Red Cross, *supra* note 161 at 632.
[240] Francesa Capone, *supra* note 165 at 748.

reverberating effects of electricity disruption, already constitutes a stronger standard in comparison to opposing orthodoxies,[241] like the DoD Manual. However, further protective options have been brought forward as plausible solutions to the conundrum of electrical systems.[242] To illustrate, Shue & Whipman's first proposed reading of the assessment, "*enhanced proportionality*", prescribes for the inclusion of the long-term effects of disruption.[243] Their second reading, ("*protective proportionality*"), goes a step further, emphasising the indispensable nature to civilians of some dual-use objects.[244] Particularly, it calls for the targeting of such infrastructure to be impermissible, unless the incidental civilian harm would not be excessive in relation to an anticipated military advantage that is "*compelling*".[245] This option, at least so far, has been the least preferred by academics.[246] In all cases, these propositions underscore a willingness for the ICC to potentially, either, broaden the scope of the effects which it accounts for as having been caused by electricity disruption, or, heighten the benchmark of proof for a State to demonstrate that it wielded an advantage in the attack. This would also facilitate encompassing attacks against electrical systems under the scope of Art.8(2)(b)(iv).

This question will be of prime importance in the coming months. Whilst finishing the writing of this Paper, the ICC issued arrest warrants for Sergei Ivanovich Kobylash, who at the relevant time was Commander of the Long-Range Aviation of the Aerospace Force, and Viktor Nikolayevich Sokolov, who was the Commander of the Black Sea Fleet. The OTP stated that these individuals bear responsibility for attacks on critical infrastructure in Ukraine, including power plants, which may have constituted war crimes within the meaning of Art.8(2)(b)(ii) and (iv).[247]

---

[241] Francesa Capone, *supra* note 165 at 752 (In her Paper, Capone proposes the adoption of the International Committee of the Red Cross' stance, although acknowledging that it is already a widely accepted standard).
[242] Francesa Capone, *supra* note 165 at 751-3.
[243] Henry Shue & David Wippman, *supra* note 209 at 570-2.
[244] Francesa Capone, *supra* note 165 at 753.
[245] Henry Shue & David Wippman, *supra* note 209 at 574.
[246] Francesa Capone, *supra* note 165 at 753.
[247] Statement by Prosecutor Karim A. A. Khan on the issuance of arrest warrants in the Situation in Ukraine, International Criminal Court (Mar. 5, 2024),

Concludingly, the ICC will need to take a stance on emerging academic debates which, regardless, have in common their advocacy for setting out a higher standard of protection which takes into account the changing role of electrical systems vis-à-vis civilians in armed conflict. Consequently, only then may the ICC be able to successfully engage the individual criminal responsibility of individuals launching attacks against electrical systems, and thereby also concretise the case against the Russian Federation for their cyber attacks.

III. Partial Conclusion

The Russo-Ukrainian conflict has placed the ICC under the spotlight to take a stance on the future of international criminal responsibility. First, the Court will need to clarify whether the Rome Statute needs amendment to address immediate concerns that state actors in cyberspace have been shielded from responsibility, and thereby determine if it has jurisdiction over cyber-enabled crimes. Second, it will need to disentangle the applicable approach to the analysis of the legality of targeting electrical systems, in order to clarify its stance on their evolving status. This interpretative endowment will unfold in the months and years to come, and this Chapter has highlighted the gaps it will need to address before it can bring a case. However, this Chapter has established that a successful prosecutorial process could be commenced against individuals launching COs on a nation's electrical grid, starting with the Russo-Ukrainian War, if these steps are addressed by the Court.

https://www.icc-cpi.int/news/statement-prosecutor-karim-aa-khan-kc-issuance-arrest-warrants-situation-ukraine.

CONCLUSIONS

Cyber operations directed against electrical infrastructure can be considered war crimes under Article 8 of the Rome Statute and, thereby, the Russian Federation's 'most responsible' actors could be investigated, and prosecuted, as war criminals, for attacking Ukraine's energy infrastructure. However, numerous challenges stand in the way of this conclusion.

To begin with, although cyber operations targeting electrical systems are bound by the norms of *Jus in Bello*, for criminal responsibility to be engaged under specified paragraphs of Article 8, the operations must rise to the level of attack. To this end, an effects-based approach will need to be followed by the International Criminal Court. For all cyber operations to be encompassed by the definition of attack, the reverberating effects of electricity disruption will need to account for the purposes of this assessment. Then, any cyber operation targeting electrical systems which harms, or attempts to harm, civilians, can cross the threshold. Otherwise, it is most likely that only destructive cyber operations qualify.

In addition, cyber operations targeting electrical systems can give rise to sufficiently grave situations to become an admissible case before the Court, yet only if they display sufficient scale and impact in attack, and if the reverberating effects of the attack are taken into account. Furthermore, this statement will be dependent on the fact that those who will likely be the object of investigation are the 'most responsible', and it is not immediately clear whether it is hackers, or their superior military commanders, the ones who bear the most responsibility. Regardless, these attacks can fall under the scope of the provisions of Article 8, notably the prohibition of attacking civilian objects, and the prohibition of carrying out disproportionate attacks, insofar as the operation is widespread and indiscriminate. This conclusion applies, equally, to cyber operations being launched alone, or in conjunction with kinetic weapons, because they may either constitute new means of committing, or otherwise contributing to the commission, of war crimes. However, the ease with which subject-matter

jurisdiction is engaged will be directly correlated to the approach which the Court takes in regard to the applicable benchmarks and interpretations.

Lastly therefore, the Court has been endowed with an interpretative role to shape the future of international criminal prosecution in the face of modern warfare. To construct a case, the Court will first need to clarify whether it can have jurisdiction over cyber-enabled crimes, or whether the Rome Statute needs amendment to get around the prohibition of analogy. Furthermore, the Court will need to ascertain the applicable standard to analyse the legality of targeting a nation's electrical systems, and this exercise will specially need to be carried in view of addressing the changing role of electricity vis-à-vis civilians' ability to survive in armed conflict.