Volume 2, Issue 2

RESEARCH ARTICLES

Cybersecurity and International Law: Charting Stability in the Black Sea–Eastern Mediterranean Region

DR GIJO GEORGE[1]

Abstract

In an era of geopolitical flux, cyberattacks have become a new battleground that intertwines state security with private life. The Black Sea and Eastern Mediterranean regions have seen aggressive cyber and electronic operations (e.g. satellite-navigation jamming of commercial vessels) used to advance strategic aims. Such stealthy conflict —from critical-infrastructure intrusions to disinformation campaigns— test the limits of existing international law. These threats often evade easy attribution and fall below the threshold of traditional armed conflict, challenging states' ability to respond. Under current public international law (the UN Charter and Geneva Conventions), the use of force is broadly prohibited, and civilian harm must be minimized. International law is incoherent with the dominance of non-state actors (hackers, firms, etc.) in cyberspace and thus has no teeth against digital aggression. The result is routine noncompliance with little accountability, which erodes trust in institutions and norms. This paper's central research question asks: can international law, as currently structured, effectively constrain cyber aggression and preserve stability in the Black Sea–Eastern Mediterranean (region), or are new legal frameworks required? The paper addresses this through a doctrinal analysis of treaties, UN resolutions, North Atlantic Treaty Organization/European Union declarations, and state cyber doctrines. The study suggests that bridging the cyber gaps is crucial to reinforcing the rule of law and preventing the erosion of international order. In the Black Sea–Eastern Mediterranean

[1] Principal and Professor of Law, Jarbom Gamlin Government Law College, Itanagar, India.

region, strengthening cyber norms would help sustain social cohesion and uphold political credibility during crises.

Keywords: cybersecurity; international law; state sovereignty; hybrid warfare; regional security

Introduction

In today's great-power rivalry and hybrid warfare, the Black Sea–Eastern Mediterranean area has emerged as a frontline. Situated between Europe, Asia and the Middle East, it is often seen as a major geopolitical hotspot, a contested zone where larger geopolitical forces play out with implications for shipping routes, energy, infrastructure and even global food security.[2] Recently this vital corridor has faced a surge of cyber and electronic attacks –from jamming satellite navigation to hacking networks and spreading disinformation– deployed secretly to advance strategic goals.[3] These activities push the boundaries of existing law. Under Article 2(4) of the UN Charter, states must refrain from the threat or use of force against the territorial integrity or political independence of any state. Concurrently, International Humanitarian Law, specifically Additional Protocol I, mandates that parties to a conflict distinguish between combatants and civilians to minimize harm to the latter.[4] Experts warn that such ambiguous aggression in the Black Sea could make all forms of security, including safe navigation and infrastructure, very uncertain.[5] Similarly, U.S. officials note that adversaries are running advanced disinformation campaigns led by Russia, China and Iran that corrode trust and threaten any progress in the region. Cyberspace has become

[2] Heinz-Jürgen Axt, *'conflicts and Global Powers in the Eastern Mediterranean. An Introduction'* (2022) 70 *Comparative Southeast European Union Studies* 393–413.

[3] Henrik Praks, *Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage* (Hybrid CoE Working Paper 32, European Union Centre of Excellence for Countering Hybrid Threats, May 2024) 17 https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf, accessed 20 September 2025.

[4] Zhifeng Jiang, 'Regulating the Use and Conduct of Cyber Operations through International Law: Challenges and Fact-finding Body Proposal' (2020) 5 *LSE Law Review* 59, 60.

[5] Christian Bueger and Tobias Liebetrau, 'Critical Maritime Infrastructure Protection: What's the Trouble?' (2023) *Marine Policy 155* 105772, 1.

a strategic battleground blending national security and private life, endangering regional stability and putting strain on traditional legal norms.[6]

The central research question of this study asks whether current international law can effectively constrain cyber aggression and preserve stability in the Black Sea–Eastern Mediterranean (region), or whether new legal frameworks are needed. Put differently: can the UN Charter's rules governing the use of force (*jus ad bellum*) and the principles of International Humanitarian Law —often referred to as the Law of Armed Conflict— apply adequately in cyberspace? Western governments (North Atlantic Treaty Organization and European Union members) tend to insist that the existing Charter-based regime covers cyber attacks.[7] In contrast, Russia and its allies have repeatedly complained that international law lacks teeth in the cyber domain and have even proposed a new binding cyber-security treaty.[8] This divergence raises practical dilemmas. For example, would a large-scale hack on a coastal nation's power grid count as an armed attack under Article 51 and trigger collective self-defense, or would it be treated as ordinary crime? Scholars warn of routine noncompliance and eroding norms if these uncertainties persist.[9]

This article uses a doctrinal legal methodology, analyzing key texts –the UN Charter, Geneva Conventions, treaties, UN resolutions, and major alliance declarations– as well as national cyber doctrine statements, to clarify how jus ad bellum and jus in bello intersect with cyber operations. The paper proceeds as follows: Section 2 surveys the regional cyber-threat landscape; Section 3 examines applicable international legal norms (the use-of-force and IHL frameworks); Section 4 identifies

[6] Samantha Bradshaw, Hannah Bailey and Philip N Howard, *Industrialized Disinformation: 2020 Global Inventory of Organised Social Media Manipulation* (Project on Computational Propaganda, Oxford Internet Institute Working Paper 2021.1, 2021) https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf, accessed 20 September 2025.

[7] Lucas Kello, 'Cyber legalism: why it fails and what to do about it' (2021) *Journal of Cybersecurity 7* tyab014, 1 https://doi.org/10.1093/cybsec/tyab014.

[8] Aleksi Kajander, *Unnecessary Repetition: Russia's Latest Attempt at a New UN Convention on Cyberspace* (North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence 2023) 1 https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/uploads/2023/08/UnnecessaryRepetitionFinalVersionExportV2-1.pdf accessed 20 September 2025.

[9] Lorraine Finlay and Christian Payne, 'The Attribution Problem and Cyber Armed Attacks' (2019) 113 *AJIL Unbound* 202 https://doi.org/10.1017/aju.2019.35 accessed 20 September 2025.

current legal gaps; Section 5 compares Western (NATO/EU) and Russian approaches; Section 6 presents a hypothetical cyber-attack case study; Section 7 suggests legal adaptations (defining cyber armed attacks and strengthening IHL in cyberspace); Section 8 reviews multilateral norm-building initiatives; and Section 9 concludes with implications and recommendations.

1. Cyber Threat Landscape in the Black Sea–Eastern Mediterranean

A. Geopolitical and Cyber Context

The Black Sea–Eastern Mediterranean region is a crossroads of competing security interests. It lies where Russia's western flank (the Black Sea) meets the Eastern Mediterranean conflicts (such as Syria and Israel–Iran tensions). Russia's full-scale war in Ukraine has turned the Black Sea into a main point of confrontation between Russia and North Atlantic Treaty Organization/European Union countries, while old disputes (for example over Cyprus and maritime boundaries) and rivalries (such as Turkey–Greece or Iran–Israel) keep the Eastern Mediterranean tense.[10] Experts describe this area as wedged between the European Union, Ukraine, Russia, Türkiye and the Caucasus, meaning any conflict there could have wide repercussions. In this environment of strategic ambiguity—frequently categorized by security analysts as a 'gray zone' between routine statecraft and open armed conflict—states increasingly employ cyber tools as part of hybrid warfare.[11] For example, in peacetime Israel–Iran confrontations or during North Atlantic Treaty Organization exercises, adversaries can quietly infiltrate networks or jam signals without open hostilities. The Internet and electronic systems have become another arena of competition: satellite communications, navigation (Global Navigation Satellite System(s)), power grids, ports and even social media can be disrupted or weaponized to gain advantage without crossing the conventional force threshold.[12] This digital front will challenge the

[10] Atlantic Council Task Force on Black Sea Security, *A Security Strategy for the Black Sea* (Atlantic Council, 15 December 2023) https://www.atlanticcouncil.org/in-depth-research-reports/report/a-security-strategy-for-the-black-sea/, accessed 20 September 2025.

[11] Amy Ormrod, David Ormrod and Jill Slay, '*Cyber Offensive Operations in Hybrid Warfare: Observations from the Russo-Ukrainian conflict'* (2023) *Journal of Information Warfare,* Vol. *22* (1), 76–87, 76.

[12] North Atlantic Treaty Organization, *Hybrid threats and hybrid warfare* (North Atlantic Treaty Organization, October 2024) https://www.North Atlantic Treaty Organization.int/North Atlantic Treaty

consistency of international law and security frameworks, because cyberattacks can cause havoc without leaving visible marks.[13]

B. Notable Cyber and Electronic Incidents

Recent years have seen illustrative examples of cyber aggression in the Black Sea–Eastern Mediterranean region. Notably, Russia has employed electronic warfare to protect its positions in the Eastern Med. Russian forces have repeatedly jammed GPS signals over Syria, Lebanon, Cyprus and surrounding waters, severely disrupting commercial navigation.[14] This Global Navigation Satellite System(s) interference in the Black Sea–Eastern Mediterranean region has threatened the safety of commercial vessels by severely disrupting their electronic navigation systems, and even degraded ships' maritime radars.[15] Similarly, a surge of false positioning signals and spoofing attacks in the Eastern Mediterranean and Persian Gulf was reported.[16] Marine authorities confirmed severe GPS disruptions affecting ships in those waters; one incident off Haifa appeared to involve a deliberate circular pattern of spoofed signals. These attacks correspond to rising regional tensions (e.g. Iran–Israel hostilities) and highlight how satellite navigation can be a target.[17]

Beyond jamming, there have been high-impact cyber intrusions on critical infrastructure. In 2015–16, coordinated cyberattacks on Ukraine's electrical grid (attributed to Russian state hackers) caused mass blackouts. According to a U.S. cybersecurity team's report, remote intruders disrupted three regional power distribution companies, impacting approximately 225,000 customers in Ukraine. The attackers used legitimate credentials and malware to open breakers and disable systems.

Organization_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf, accessed 20 September 2025.

[13] FP Analytics, *Digital Front Lines* (FP Analytics, 2023) https://digitalfrontlines.io/, accessed 20 September 2025.

[14] C4ADS, *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria* (C4ADS 2019) 3 https://c4ads.org/wp-content/uploads/2022/05/AbovEuropean UnionsOnlyStars-Report.pdf, accessed 20 September 2025.

[15] Andrej Androjna, Tanja Brcko, Ivica Pavic and Harm Greidanus, 'Assessing Cyber Challenges of Maritime Navigation' (2020) *J Mar Sci Eng,* Vol. *8 (10),* 776.

[16] F Jiguet *et al*, 'Global Navigation Satellite System(s) spoofing in conflict zones disrupts wildlife tracking and hampers research and conservation efforts' (2025) *Nat Commun* 16, 1199.

[17] Cheng Lu, Zukun Lu, Zhe Liu, Long Huang and Feiqiang Chen, 'Overview of satellite nav spoofing and anti-spoofing techniques' (2024) *Frontiers in Physics 12* 1428544,.

This incident demonstrated that cyber weapons can have physical effects on utilities.[18] More recently, adversaries have used distributed-denial-of-service and defacement attacks as political tools. Pro-Russian hacktivist groups (e.g. KillNet, NoName, the so-called IT Army of Russia) have launched coordinated Distributed Denial of Service campaigns and website defacements against Ukrainian and allied targets.[19] Conversely, Ukrainian-affiliated IT Army volunteers have struck back at Russian government and military sites in a hybrid form of retaliation.[20]

Information operations are also a major factor. Russian and allied actors frequently carry out disinformation and influence campaigns aimed at countries in the Black Sea–Eastern Mediterranean region.[21] U.S. officials warn that these advanced disinformation efforts, spearheaded by Russia, threaten to undermine progress in the Black Sea area.[22] For example, social media stories have been used to sway public opinion about the conflicts in Syria or migrant crises in the Balkans.[23] The cyber dimension of security in this region is already active and diverse: electronic jamming, network intrusions, hacktivism and disinformation all combine as ambiguous tactics. However, legal experts note that disinformation rarely meets the threshold of a use of force or armed conflict unless it causes physical consequences, thus occupying a regulatory gap.[24]

---

[18] Doney Abraham, Siv Hilde Houmb and Laszlo Erdodi, 'Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation' (2025) *Applied Sciences 15* 9233, 9233.

[19] US Department of Health & Human Services, Health Sector Cybersecurity Coordination Center (HC3), '*Pro-Russian Hacktivist Group "KillNet" Threat to HPH Sector', HC3*, 30 January 2023, 1 https://www.hhs.gov/sites/default/files/russian-threat-actors-targeting-the-hph-sector-tlpclear.pdf, accessed 20 September 2025.

[20] Anna Lysenko and Seva Gunitsky, 'The invisible front: Ukraine's IT army and the evolution of cyber resistance' (2025) *41 Post-Soviet Affairs* 263–288, 263.

[21] Natalie Sabanadze and Galip Dalay, '*Understanding Russia's Black Sea strategy: How to strengthen European Unionrope and North Atlantic Treaty Organization's approach to the region',* Chatham House Research Paper, 28 July 2025, 16 https://www.chathamhouse.org/2025/07/understanding-russias-black-sea-strategy, accessed 20 September 2025.

[22] Centre for Strategic and International Studies (CSIS), 'Navigating Security Challenges in the Black Sea Region', *Transcript, CSIS*, 11 January 2024, 1 https://www.csis.org/analysis/navigating-security-challenges-black-sea-region, accessed 20 September 2025.

[23] Anna Triandafyllidou and Stein Monteiro, 'Migration narratives on social media: Digital racism and subversive migrant subjectivities' (2024) *First Monday,* Vol. 29 (8), 13 .

[24] Benjamin Jensen, Brandon Valeriano and Sam Whitt, 'How cyber operations can reduce escalation pressures: Evidence from an experimental wargame study' (2024) 61 *Journal of Peace Research* 119, 1.

C. Key Actors and Vulnerabilities

The main state actors in this area are the coastal countries and other regional powers. These include Russia, Turkey, Greece, Ukraine, Romania, Bulgaria, Cyprus, Israel, Iran and others. Many of these countries (Turkey, Greece, Romania, Bulgaria and soon Ukraine) are members of North Atlantic Treaty Organization or the European Union and follow Western cyber-defense approaches.[25] Russia remains the most aggressive cyber adversary in the Black Sea region, employing both official forces and proxy groups.[26] Research highlights that Russia's cyber network is extensive, complex and often opaque. It mixes federal security services with government-tolerated hackers, cybercriminal rings and even private military companies.[27] Russian patriotic hackers and state security agencies, cybercriminals and private military companies blend together to create the Russian cyber web.[28] This multidirectional ecosystem – ranging from Russia's Federal Security Service (Federal'naya sluzhba bezopasnosti)/Russia's Main Intelligence Directorate (Glavnoye razvedyvatel'noye upravlenie) operations to volunteer hacktivists (KillNet, Advanced Persistent Threat groups, etc.) – makes attribution difficult and increases Russia's cyber reach.[29] Turkey also engages actively: its armed forces and intelligence services conduct cyber reconnaissance and defensive operations in the Eastern Med (especially around contested waters and energy

[25] Yavor Todorov, 'Navigating Uncharted Waters: Tackling Maritime Cybersecurity Challenges in the Black Sea Region' (2024) *Information & Security: An International Journal,* Vol. *55* (2), 113–132, 113.
[26] Sabanadze and Dalay (n 20).
[27] Justin Sherman, '*Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior', Atlantic Council*, 19 September 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/, accessed 20 September 2025.
[28] Justin Sherman, 'Unpacking Russia's cyber nesting doll', *Atlantic Council*, 20 May 2025, https://www.atlanticcouncil.org/content-series/russia-tomorrow/unpacking-russias-cyber-nesting-doll/, accessed 20 September 2025.
[29] Annegret Bendiek, Jakob Bund and Mika Kerttunen, 'The Attribution Dividend: Protecting Critical Infrastructure from Cyber Attacks', SWP Comment 2024/C 46, 9 October 2024, https://www.swp-berlin.org/10.18449/2024C46/, accessed 20 September 2025.

exploration).[30] Iran, Israel and Gulf states have also sharpened their cyber capabilities as tensions rise.[31]

Non-state actors and proxies magnify these threats. In Russia's orbit, hacktivist collectives (KillNet, NoName, Anonymous Sudan proxies, etc.) freely target rival states.[32] Conversely, nationalist hacktivists in Ukraine, Greece, and elsewhere have arisen. Criminal organizations also play a role; for example, cybercriminal gangs may cooperate with, or be coerced by, state agencies.[33] Commercial hackers-for-hire and so-called patriotic 'hackers' can serve as covert force multipliers. Both sides increasingly weaponize dual-use technology: maritime GPS, telecom satellites, undersea cables and civilian internet infrastructure can become vulnerable nodes.[34] Critical sectors at risk include energy (electric grids, pipelines), transportation (ports, logistics networks, shipping), telecommunications (Internet Service Providers, cell networks, satellite comms), and finance. For example, a denial-of-service attack or malware incident targeting a port authority or maritime traffic control system could bring commerce to a standstill.[35] Civilian networks often carry both military and public communications, which means that dual-use cyber infrastructure can become a point of conflict. Under international humanitarian law, such infrastructure is a military target only if it meets

[30] International Institute for Strategic Studies, 'Turkiye' in *Cyber Capabilities and National Power Vol. 2*, Research Paper, International Institute for Strategic Studies, September 2023, 141 https://www.iiss.org/globalassets/media-library---content---migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_12-turkiye.pdf, accessed 20 September 2025.

[31] Ibid.

[32] Julia Dickson and Emily Harding, 'How a Cyber Alliance Took Down Russian Cybercrime"', C*enter for Strategic and International Studies*, 28 July 2025, https://www.csis.org/analysis/how-cyber-alliance-took-down-russian-cybercrime, accessed 20 September 2025.

[33] Janine Schmoldt, 'Cyber proxies: covert state–non-state interactions in cyberwarfare', in Tim Stevens and Joe Devanny (eds), *Research Handbook on Cyberwarfare* (Cheltenham: Edward Elgar Publishing, 2024) 131–47, 132.

[34] A Ertan, K Floyd, P Pernik and T Stevens (eds), *Cyber Threats and North Atlantic Treaty Organization 2030: Horizon Scanning and Analysis* (North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization) Publications, 2020), https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/uploads/2020/12/Cyber-Threats-and-North Atlantic Treaty Organization-2030_Horizon-Scanning-and-Analysis.pdf, accessed 20 September 2025.

[35] M. V. Clavijo Mesa, C. E. Patino-Rodriguez and F. J. Guevara Carazas, 'Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains' (2024) *Information 15,* 710.

strict criteria.[36] Overall, the Black Sea–Eastern Mediterranean region's strategic importance – from oil and gas routes to key ports and information points.[37]

3. International Legal Framework for Cyber Operations

A. UN Charter: Use of Force and Self-Defense

International law's starting point is the UN Charter. Article 2(4) prohibits the threat or use of force by states, a foundational rule presumed to apply across domains.[38] In 2013 a UN Group of Governmental Experts explicitly affirmed that international law, and in particular the Charter of the United Nations, is applicable to the use of information and communications technologies.[39] Likewise, North Atlantic Treaty Organization and European Union statements now affirm that cyber operations are governed by the same jus ad bellum norms as conventional force.[40] Notably, North Atlantic Treaty Organization's 2014 Wales Summit Declaration recognized that the use of cyber capabilities could, if used in a manner that meets the threshold of an 'armed attack' under Article 51 of the UN Charter, could lead to the invocation of Article 5 of the North Atlantic Treaty (collective defense).[41] This means a cyber-attack whose effects are comparable to those of a conventional armed attack could trigger the Charter's self-defense rule.[42] Indeed, North Atlantic Treaty Organization officials have emphasized that cyber defense is a core mission and that a cyber attack could be

[36] International Committee of the Red Cross, '*International Humanitarian Law and Cyber Operations during Armed conflicts',* International Committee of the Red Cross position paper, November 2019, https://www.International Committee of the Red Cross.org/sites/default/files/document/file_list/International Committee of the Red Cross_International Humanitarian Law-and-cyber-operations-during-armed-conflicts.pdf, accessed 20 September 2025.

[37] Atlantic Council Task Force on Black Sea Security (n 9).

[38] Michael N Schmitt, 'Cyberspace and the Jus ad Bellum: the State of Play' (2024) *International Law Studies 103,* 195.

[39] Harriet Moynihan, '*The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention',* Chatham House Research Paper, 29 November 2019, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf, accessed 20 September 2025.

[40] Schmitt and Pakkam (n 37).

[41] Joe Burton and Tim Stevens, '4 System, Alliance, Domain: A Three-Frame Analysis of North Atlantic Treaty Organization's Contribution to Cyber Stability' in Robert Chesney (ed), *Cyberspace and Instability* (Edinburgh: Edinburgh University Press 2022), 129–52, 133.

[42] Schmitt and Pakkam (n 37).

grounds for invoking Article 5, provided the cyber assault causes sufficiently grave damage.[43]

At the same time, there are uncertainties in the law. The concept of "use of force" in Article 2(4) of the UN Charter was originally drafted with guns and bombs in mind, so applying it to digital attacks is debated.[44] Some scholars suggest an effects-based test, meaning only cyber operations that cause actual physical harm or destruction should count as the use of force.[45] Others argue that crippling a country's critical infrastructure (like its power grid, dams or nuclear plants) could itself be considered an armed attack if it causes physical damage.[46] On this point, the Tallinn Manual 2.0 (a well-known but nonbinding study) and many experts say that the scale of consequences matters. Cyber actions that result in death, injury or substantial property damage likely qualify as use of force and even as an armed attack under Article 51, while mere espionage or data theft would not.[47] The U.S. and North Atlantic Treaty Organization have similarly indicated that a cyber attack causing casualties or major destruction could be treated like an armed attack that justifies self-defense. However, in ambiguous cases – for example, an espionage intrusion or a ransomware hack – the threshold for force is usually not reached.[48]

If a cyber operation does amount to an armed attack, the right of self-defense under Article 51 of the UN Charter is triggered.[49] That means victim states may lawfully defend themselves – individually or collectively – against the attacker. Western countries maintain that Article 51 applies to cyber attacks in no other case than this: i.e.

[43] North Atlantic Treaty Organization, 'Cyber defence', https://www.North Atlantic Treaty Organization.int/cps/en/North Atlantic Treaty Organizationhq/topics_78170.htm, accessed 20 September 2025.
[44] Schmitt and Pakkam (n 37).
[45] Thomas Eaton, 'Self-Defense to Cyber Force: Combatting the Notion of "Scale And Effect"' (2021) *36 American University International Law Review,* 697.
[46] Samuli Haataja, 'Cyber operations against critical infrastructure under norms of responsible state behaviour and international law' (2023) *International Journal of Law and Information Technology,* Vol. 30 (4), 423.
[47] Schmitt and Pakkam (n 37).
[48] F. Oorsprong, P. Ducheine and P. Pijpers, 'Cyber-attacks and the right of self-defense: a case study of the Netherlands' (2023) *6 Policy Design and Practice,* 217.
[49] International Committee of the Red Cross, 'International humanitarian law and cyber operations during armed conflicts' (2020) *102 International Review of the Red Cross,* 481.

when the attack reaches the armed-attack level.[50] The North Atlantic Treaty Organization policy line is consistent: Article 5 can be invoked if and when a cyber attack causes extensive destruction, injury or death akin to a kinetic assault.[51] North Atlantic Treaty Organization deliberately keeps thresholds ambiguous: as its officials note, setting clear numbers could reveal their red lines and weaken deterrence. In contrast, Russia has recently questioned whether any consensus exists on classifying malicious cyber operations as armed attacks under Article 51.[52] In UN working groups, Russia and some others have even argued that International Humanitarian Law does not automatically apply in cyberspace.[53] This dispute underscores the tension: Western allies favor extending traditional self-defense law to cover cyber aggression, while Russia suggests new rules might be needed.[54]

B. International Humanitarian Law

When cyber operations occur in an armed conflict, the law of armed conflict (International Humanitarian Law) governs their conduct.[55] The core International Humanitarian Law principles—distinction (targeting only military objectives), proportionality (weighing military advantage against collateral damage), and precaution (active measures to spare civilians)—are generally understood to apply in cyberspace, as affirmed by the 2015 (UN) Group of Governmental Experts report.[56] The International Committee of the Red Cross emphasizes that even cyber attacks must at all times distinguish between military and civilian targets.[57] Thus, cyber operations may only be directed against combatants or military objectives; attacks on civilians or

[50] Michael N Schmitt, 'Cyber Symposium – *The Evolution of Cyber Jus ad Bellum Thresholds*', *Lieber Institute for Law and Warfare*, 28 July 2022, https://lieber.westpoint.edu/evolution-cyber-jus-ad-bellum-thresholds/, accessed 20 September 2025.
[51] North Atlantic Treaty Organization (n 42).
[52] Kajander, *Unnecessary Repetition* (n 7).
[53] Ibid.
[54] Ibid.
[55] Michael N Schmitt, 'Wired warfare 3.0: Protecting the civilian population during cyber operations' (2019) 101 *International Review of the Red Cross,* 333–355, 334.
[56] International Committee of the Red Cross (n 48).
[57] L. Gisel, T Rodenhäuser and K. Dörmann, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' (2020) 102 *International Review of the Red Cross,* 287–334, 289.

purely civilian objects are prohibited.[58] This is challenging in practice because Information and Communications Technology infrastructure is often dual-use. For example, a satellite or undersea cable may carry both civilian data and military communications. International Humanitarian Law treats such an object as a military objective only if (a) its use makes an effective contribution to military action, and (b) its damage offers a definite military advantage. Otherwise it remains protected.[59] In concrete terms, hacking a power plant to create tactical advantage must still not kill civilians or destroy humanitarian services, and indiscriminate or unfocused cyber attacks are forbidden.[60]

Proportionality imposes a similar constraint. Even if a target is legitimate, an attack is unlawful if the expected civilian harm is excessive relative to the anticipated military gain.[61] The International Committee of the Red Cross notes that in the interconnected Information and Communications Technology environment, some incidental harm to civilian networks is almost inevitable, but this does not suspend the proportionality rule.[62] For example, if an aggressor state launches malware that disables an enemy's air defense radar (a military objective), but it also cripples civilian air-traffic control and causes major collateral damage, that might be disproportionate. Likewise, an attack that floods a city's electric grid to hamper military rail transport (arguably a dual-use target) would likely exceed proportionality bounds due to civilian suffering.[63] Cyber actors must also take precautions to minimize harm (Article 57 Additional Protocol I (to the 1949 Geneva Conventions)), such as using precision malware or time delays.[64] The foundational International Humanitarian Law rules limiting civilian harm carry over to cyber warfare, though their application can be complex when effects are non-physical or systemic.[65]

---

[58] Schmitt (n 54).
[59] Sophie Ryan, 'Submarine Communication Cables and Belligerent Rights in Armed conflict' (2024) 38 *Ocean Yearbook,* 459, 459–503, 460.
[60] International Committee of the Red Cross (n 35).
[61] Maxime Nijs, 'Humanizing siege warfare: Applying the principle of proportionality to sieges' (2020) *International Review of the Red Cross, Vol.* 102 (914), 683–704.
[62] International Committee of the Red Cross (n 35).
[63] Schmitt (n 54).
[64] Ibid.
[65] International Committee of the Red Cross (n 48).

C. Other Normative Developments

Beyond treaty law, various expert bodies have reaffirmed that existing international law is fully applicable to cyber operations.[66] The Tallinn Manuals on cyber warfare (first edition 2013, second 2017) are not binding law, but they compile authoritative interpretations by international law scholars.[67] They proceed on the assumption that jus ad bellum and International Humanitarian Law apply to cyberspace, subject to technical nuance (e.g. use of force requires physical effects). Likewise, the 2013 (UN) Group of Governmental Experts report on cyber norms declared that the use of information and communications technologies must adhere to the Charter.[68] The 2021 (UN) Group of Governmental Experts and Open-Ended Working Group (at the UN) reports reaffirmed this stance: the 2021 (UN) Group of Governmental Experts explicitly stated that international law, in particular the UN Charter, in its entirety applies to the information and communications environment.[69] The (UN) Group of Governmental Experts also identified International Humanitarian Law principles like distinction and proportionality as established international legal principles for cyber warfare, though it noted further study was needed on implementation.[70] Most states on the UN stage have endorsed these conclusions, repeatedly affirming that cyberspace is not a lawless arena.[71]

In late 2024 the European Union Council went further by unanimously adopting a declaration that international law fully applies to cyberspace.[72] The declaration underscores that the UN framework of responsible state behavior – grounded in the Charter, human rights law and International Humanitarian Law – remains essential for

[66] Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc **A/76/135** (14 July 2021) para 2.
[67] Ori Pomson, 'Methodology of identifying customary international law applicable to cyber activities' (2023) *Leiden Journal of International Law* **36,** 1023–1047, 1026.
[68] Schmitt and Pakkam (n 37).
[69] UN Group of Governmental Experts Report on Responsible State Behaviour (n 65), para 69.
[70] Ibid, para 71(f).
[71] Michael N Schmitt, 'Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace' (2020) 3 *Texas National Security Review* 32.
[72] Council of the European Union, '*Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace'*, ST-15833-2024-INIT, 18 November 2024, https://data.consilium.European_Unionropa.European_Union/doc/document/ST-15833-2024-INIT/en/pdf, accessed 20 September 2025.

cyber stability.[73] In other words, European Union states officially embrace the mainstream view that no new jus ad bellum regime is needed: rather, they pledge to clarify and implement how existing obligations reach digital activities.[74] Similarly, leading countries (the U.S., North Atlantic Treaty Organization members) have published cyber doctrine positions affirming that all armed conflict rules and self-defense rights in the Charter are unaffected by the medium of cyber.[75] For instance, the U.S. National Cyber Strategy and legal policies emphasize that states must abide by UN law in cyberspace.[76] In contrast, Russia's governments have repeatedly proposed new binding cyber treaties and hinted that current law does not satisfactorily address cyber threats.[77] In UN forums, Russia has at times caused a stir by questioning the applicability of International Humanitarian Law to peacetime cyber operations and arguing there is no consensus on whether cyber attacks qualify as armed attacks.[78] These positions reflect a desire by some actors to negotiate new international rules on cybersecurity, whereas most Western states prefer to build consensus around existing legal norms.

Overall, the authoritative trend is clear: leading analyses (Tallinn Manuals, UN expert reports) assume that pre-existing legal principles govern state cyber conduct.[79] The prevailing interpretation among North Atlantic Treaty Organization/European Union members is that law's broad ban on force and requirement to protect civilians extends into cyberspace.[80] What remains unsettled is how to operationalize these principles – e.g. by developing clearer definitions of armed attack in cyber terms,

[73] Harriet Moynihan, 'The vital role of international law in the framework for responsible state behaviour in cyberspace' (2021) *Journal of Cyber Policy,* Vol. 6 (3), 394–410, 397.
[74] Schmitt and Pakkam (n 37).
[75] Schmitt (n 70).
[76] The White House, '*National Cybersecurity Strategy',* 1 March 2023,https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, accessed 21 September 2025.
[77] Lauren Zabierek, Christie Lawrence, Miles NEuropean Unionmann and Pavel Sharikov, '*US-Russian Contention in Cyberspace', Belfer Center for Science and International Affairs*, Harvard Kennedy School, June 2021, https://www.belfercenter.org/publication/us-russian-contention-cyberspace, accessed 20 September 2025.
[78] Kajander, *Unnecessary Repetition* (n 7).
[79] François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press, 2020), 353–76, 364.
[80] Gisel, Rodenhauser and Dörmann (n 56).

setting standards for attribution, and agreeing on mutual cyber assistance.[81] But the message of the international community (UN, International Committee of the Red Cross, allied declarations) is that there is no need to reinvent law a priori; rather, states should adapt the current framework to the unique features of cyber operations.[82]

D. Regional Alliances and Collective Defense

Regional security organizations have explicitly extended collective defense concepts to cover cyber threats. North Atlantic Treaty Organization has been at the forefront: already in 2014 it declared that cyber defense is part of its core task of collective defense, meaning that a cyber attack could, in principle, trigger Article 5.[83] At the Wales Summit, Allies acknowledged that the scope of Article 5 could encompass cyber incidents depending on effects, and they later reaffirmed cyber as a distinct operational domain (2016 Warsaw Summit).[84] The Brussels Communiqué (2021) reiterated that a cyber aggression could invoke Article 5, but that decisions must be made case-by-case.[85] This means North Atlantic Treaty Organization will consider a cyberattack on a member state just as it would any attack: it will assist the Party or Parties so attacked such action as it deems necessary under Article 5.[86] The only difference is one of ambiguity: Allied leaders purposely avoid publicizing the threshold for cyber trigger, thereby deterring adversaries by leaving them uncertain. North Atlantic Treaty Organization's position – blurry but consistent – is that effects comparable to 2007 Estonia or 9/11 could justify collective response, but no fixed line is given.[87]

[81] Finlay and Payne (n 8).
[82] International Committee of the Red Cross (n 35).
[83] North Atlantic Treaty Organization (n 42).
[84] Sarah Wiedemar, '*North Atlantic Treaty Organization and Article 5 in Cyberspace', CSS Analyses in Security Policy* No 323, Center for Security Studies, ETH Zürich, May 2023, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse324-EN.pdf, accessed 20 September 2025.
[85] Ibid.
[86] Ibid.
[87] Michaela Prucková, 'Cyber attacks and Article 5 – a note on a blurry but consistent position of North Atlantic Treaty Organization', *North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence*, 2021 https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-North Atlantic Treaty Organization/, accessed 20 September 2025.

The European Union, which has its own mutual defense clause (Article 42(7) Treaty on European Union), likewise extends legal protections to cyberspace.[88] European Union Member States have adopted a common understanding affirming that the UN framework (Charter, International Humanitarian Law, etc.) fully applies in cyberspace.[89] The European Union cyber diplomacy vision links hard defense (e.g. cybercrime law enforcement, Computer Emergency Response Team cooperation) with soft-power norms building.[90] The European Union has also emphasized cooperative measures – joint cyber exercises, information sharing, and capacity building – to buttress Black Sea–Eastern Mediterranean (region) stability.[91]

At the national level, Black Sea–Eastern Mediterranean (region) countries generally align with these alliance policies. North Atlantic Treaty Organization members like Turkey, Romania, Bulgaria and Greece incorporate the UN Charter's principles into their cyber strategies (often citing North Atlantic Treaty Organization doctrine and European Union law).[92] For instance, Turkey's 2016 Cybersecurity Strategy calls on all actors (individuals and the state) to fulfil all legal responsibilities in providing cyber security.[93] Ukraine, even before full European Union/North Atlantic Treaty Organization accession, regards cyber attacks from Russia as acts of war

[88] Aistė Mickonytė, 'Obligation to Mutual Assistance Under Article 42(7) Treaty on European Union: The Conundrum of Intentional Ambiguity' (2024) *ICL Journal, Vol. 18,* 311–338, 315.

[89] Council of the European Union, *Declaration on a Common Understanding of International Law in Cyberspace*, ST 15833/24, 18 November 2024, https://data.consilium.European Unionropa.European Union/doc/document/ST-15833-2024-INIT/en/pdf, accessed 20 September 2025.

[90] T. Lațici, '*Understanding the European Union's approach to cyber diplomacy and cyber defence'*, European Unionropean Parliamentary Research Service, Briefing PE 651.937, May 2020, https://www.European Unionroparl.European Unionropa.European Union/RegData/etudes/BRIE/2020/651937/EPRS_BRI%282020%29651937_EN.pdf, accessed 20 September 2025.

[91] European Unionropean Commission and High Representative of the Union for Foreign Affairs and Security Policy, *The European Union's strategic approach to the Black Sea region*, Joint Communication JOIN(2025) 135 final, Brussels, 28 May 2025, https://enlargement.ec.European Unionropa.European Union/document/download/170d9b3a-d45f-4169-80fa-9adb753c0921_en?filename=European Union+Strategic+Approach+Black+Sea+Strategy.pdf.

[92] Emre Halisdemir, '*National Cybersecurity Organisation: TURKEY', North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence*, Tallinn 2021, https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/uploads/2021/08/TUR_country_report_final_clean_ver_2408.pdf, accessed 20 September 2025.

[93] Nezir Akyeşilmen, 'Türkiye in the Global Cybersecurity Arena: Strategies in Theory and Practice' (2022) *Insight Turkey, Vol. 2*4 (3), 109, 111.

requiring military-grade responses.[94] The bloc of Western-aligned states in the region stresses that international law's use-of-force and collective defense rules apply in cyberspace. Russia, on the other hand, while still formally acknowledging some charter norms, continues to push for a treaty that it believes would give it more leverage.[95] This split in rhetoric reflects the broader question: whether to work within the existing legal order (with improvements) or to renegotiate it. For Black Sea–Eastern Mediterranean (region) security, most stakeholders have so far opted for the former path.

4. Gaps and Challenges in the Current Legal Regime

A. Absence of a dedicated cyber treaty

Cyberspace currently has no analogue to the nuclear or chemical arms-control regimes, leaving a significant legal lacuna.[96] States rely on general UN Charter prohibitions against force and existing humanitarian law, but there is no bespoke treaty on cyber-weapons or cyberwar.[97] Attempts to create one have floundered on technical and political grounds. A treaty demands that states quantify or monitor capabilities (easy with nukes or tons of gas, impossible with virtual weapons), agree on the effects of technology (rapid, unpredictable innovation in IT), and verify compliance (cyber tools are often dual-use and covert).[98] The cyber domain's intangibility and speed undermine conventional arms-control approaches. Critics therefore warn that any treaty could be obsolete by the time it is adopted.[99]

Nonetheless, proposals for a cyber-specific accord have been floated. One approach is a multilateral information security or cyber arms-control treaty.[100] Russia

[94] Decree of the President of Ukraine No 447/2021, 26 August 2021, *On the Cybersecurity Strategy of Ukraine,* National Security and Defense Council of Ukraine.https://www.rnbo.gov.ua/en/Diialnist/4976.html, accessed 20 September 2025.
[95] Kajander, *Unnecessary Repetition* (n 7).
[96] T Reinhold, H Pleil and C REuropean Unionter, 'Challenges for Cyber Arms Control: A Qualitative Expert Interview Study' (2023) 16 *Zeitschrift für Außen- und Sicherheitspolitik* 289, 293.
[97] Gisel, Rodenhauser and Dörmann (n 56).
[98] Przemysław Roguski, '*An Inspection Regime for Cyber Weapons: A Challenge Too Far?'* (2021) 115 *American Journal of International Law Unbound,* 111–115, 114.
[99] Reinhold, Pleil and REuropean Unionter (n 95).
[100] Ibid.

(supported by China and others) has repeatedly advocated negotiating a binding cybersecurity convention – arguing that existing law needs clarification and supplementation.[101] In 2018–20, Russian drafts in the UN sought an international legally binding agreement for information security. Other ideas include confidence-building measures and voluntary codes of conduct as interim steps.[102] For instance, the European Union is pursuing a UN Programme of Action on responsible state behavior in cyberspace, aiming to strengthen norms through dialogue rather than a new treaty.[103] These mixed proposals – from hard law to soft law – reflect the debate: some experts urge a traditional arms-control framework for cyberspace, while others stress flexible, behavioral regulations to address the unique challenges.[104]

B. Attribution and enforcement difficulties

A core practical gap in cyber law is attribution. Unlike a missile launch, a cyberattack can be routed through third-party servers or disguised via malware, making it extremely hard to trace the culprit.[105] Identifying the state or group behind an intrusion is sometimes difficult and often requires extensive technical intelligence. Because attackers can hide behind proxy networks, states rarely have incontrovertible proof.[106] Even when evidence is strong, the lack of a global enforcement mechanism means responses are piecemeal. victims typically resort to ad hoc measures: private incident response teams, unilateral indictments of hackers, or targeted sanctions. There

[101] Arun Sukumar and Arindrajit Basu, 'Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order' (2024) *Journal of Cyber Policy,* Vol. *9* (2), 256, 259.

[102] Kajander, *Unnecessary Repetition* (n 7).

[103] Council of the European Union, 'Cyberspace: Council approves declaration on a common understanding of application of international law to cyberspace', Press release, 18 November 2024, https://www.consilium.European Unionropa.European Union/en/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/, accessed 20 September 2025.

[104] Reinhold, Pleil and REuropean Unionter (n 95).

[105] William C Banks, 'The Bumpy Road to a Meaningful International Law of Cyber Attribution' (2019) 113 *American Journal of International Law* (AJIL Unbound), 191–196, 195 https://doi.org/10.1017/aju.2019.32.

[106] Florian J. Egloff, 'Public attribution of cyber intrusions' (2020) *Journal of Cybersecurity,* Vol. 6 (1).

is no international cyber-Gendarmerie or agreed process to investigate transnational hacks.[107]

The consequence is a patchwork of responses. Some like-minded countries (notably the Five Eyes) publicly attribute major incidents and impose coordinated sanctions, but these actions are political, not judicial, and do not bind all states. It is usually difficult for the victim to hold the wrongdoing State accountable for cyber-operations.[108] The result is that many cyber intrusions go unpunished. Cyber criminals and state-aligned hackers often operate with relative impunity, knowing that even if detected they may face only reprisal by a few states.[109] This attribution hurdle thus undermines any consistent enforcement of international law.

C. State-centric law vs. non-state actors

Traditional international law is built around state actors, but cyberspace is dominated by non-state entities – hacktivists, criminal gangs, and multinational tech companies.[110] This dissonance renders the law incoherent with the dominance of non-state actors in cyberspace.[111] States negotiate treaties and resolve disputes with each other, but a cyberattack can originate from an independent hacker group or even a private corporation.[112] These actors are not straightforwardly controlled by governments, so the usual state-to-state law framework lacks teeth to rein them in.

Moreover, non-state actors often fill gaps left by governments. For example, large tech firms have become de facto norm-setters and responders: they can negotiate cybersecurity standards, patch vulnerabilities, and even attribute attacks (e.g. naming

[107] Dennis Broeders, 'Private active cyber defense and (international) cyber security—pushing the line?' (2021) *Journal of Cybersecurity,* Vol. *7* (1).
[108] Delerue (n 78).
[109] Egloff (n 106).
[110] A Sukumar, D Broeders and M Kello, 'The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy' (2024) *Contemporary Security Policy,* Vol 45 (1), 7, 16.
[111] Katagiri Nori, 'Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks' (2021) *Journal of Cybersecurity,* Vol. 7 (1).
[112] Finlay and Payne (n 8).

which malware was used).[113] In this fragmented landscape, powerful private cybersecurity companies or norm entrepreneurs can shape outcomes in ways the formal international legal system cannot.[114] States themselves sometimes act indirectly via proxies or volunteer hacker organizations. The state-centric design of international law struggles to capture these realities; the law provides no direct sanction against an independent hacker collective, and any state responsibility hinges on proving that the state itself directed or controlled the attack.[115]

D. Norm erosion and compliance

These gaps together contribute to an ongoing erosion of legal norms. Because cyber attackers rarely face clear consequences, a culture of noncompliance has emerged.[116] The toothlessness of the legal framework makes noncompliance, practical and cyber operations pain-free for perpetrators.[117] States routinely ignore or reinterpret rules. High-profile cases – from Russia's cyber-interference in Ukraine to persistent intellectual-property theft by other powers – test the limits of the law with little accountability.[118] Over time this undermines confidence in international institutions. When major powers flout cyber norms without censure, smaller states lose faith that the legal rules of the road have any bite.[119] The resultant atmosphere of impunity and distrust erodes the very notion of a stable, law-based digital order.

[113] S Romanosky and B Boudreaux, 'Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government' (2020) 34 *International Journal of Intelligence and CounterIntelligence* 463–493, 468.

[114] Robert Gorwa and Anton Peez, 'Big Tech Hits the Diplomatic Circuit: Norm entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord' in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behaviour, Power and Diplomacy* (Lanham, MD: Rowman & Littlefield, 2020) 283–304, 291 https://osf.io/g56c9/ accessed 20 September 2025.

[115] Justin Key Canfil, 'The Illogic of Plausible Deniability: Why Proxy conflict in Cyberspace May No Longer Pay' (2022) *Journal of Cybersecurity,* Vol. 8 (1).

[116] N Katagiri, 'Why international law and norms do little in preventing non-state cyber attacks' (2021) *Journal of Cybersecurity,* Vol. 7 (1).

[117] Nori Katagiri, 'Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks' (2021) *Journal of Cybersecurity,* Vol. 7 (1).

[118] Kristen E Eichensehr, 'Ukraine, Cyberattacks, and the Lessons for International Law' (2022) 116 *American Journal of International Law* 145, 145–49, 148.

[119] Kello (n 6).

5. Divergent State Approaches to Cyber Norms

A. Western/North Atlantic Treaty Organization/European Union perspective

The United States, European Union members and other North Atlantic Treaty Organization allies generally maintain that existing international law – especially the UN Charter – already governs cyberconflict.[120] In the view of Western governments, Article 2(4)'s prohibition on the use of force applies fully to cyberoperations, and Article 51's self-defense right can be invoked if a cyberattack rises to the level of an armed attack.[121] Western statements routinely reaffirm this stance. For example, North Atlantic Treaty Organization leaders declared in 2014 that international law, including international humanitarian law and the UN Charter, applies in cyberspace.[122] They emphasized that cyber defense is a core part of collective defense, even if decisions to invoke Article 5 (collective self-defense) would be made on a case-by-case basis.[123] Similarly, the UN Group of Governmental Experts in 2013 (including the U.S. and European Union states) stated that the Charter of the United Nations is applicable to state Information and Communications Technology operations.[124]

The European Union has echoed this interpretation. In November 2024, the European Union and its Member States approved a common declaration reaffirming that international law particularly the UN Charter fully applies to cyberspace.[125] This declaration explicitly rejects the idea that cyberspace is a legal vacuum: it asserts that cyberspace is governed by the UN framework of responsible state behaviour, emphasizing that states must obey long-standing rules even in digital operations.[126] In practice, Western allies tend to focus on clarifying how existing law applies (for instance, what level of cyber-kinetic effect qualifies as a use of force) rather than

[120] Security Council, '*Record of the open debate on Maintenance of international peace and security: cybersecurity'*, UN Doc S/2021/621, 1 July 2021, https://docs.un.org/en/S/2021/621, accessed 20 September 2025.
[121] Schmitt and Pakkam (n 37).
[122] Kubo Mačák, 'Unblurring the lines: military cyber operations and international law' (2021) 6 *Journal of Cyber Policy* 411, 413.
[123] Prucková (n 86).
[124] UN Group of Governmental Experts Report on Responsible State Behaviour (n 65).
[125] Council of the European Union (n 71).
[126] Moynihan (n 72).

writing new treaties.[127] Toward that end, North Atlantic Treaty Organization has commissioned restatements like the Tallinn Manual, and the European Union is supporting UN-based confidence and capacity building through the ongoing Programme of Action (PoA) process.[128] Western policy privileges an incremental approach: maintain the current UN framework, while refining definitions of armed attack in cyber context, rather than fundamentally rewriting the rules.[129]

B. Russia and allies' stance

By contrast, Russia (backed by some partner states) contends that the current legal framework is inadequate to address cyber threats. Since the early 2010s, Moscow has argued repeatedly for a new binding treaty on state conduct in cyberspace. In its UN statements, Russia frames this not as a rejection of international law, but as a necessary clarification and extension of it.[130] Russia presented a cyber treaty as a critical means to clarify how existing international law applies and to introduce additional norms.[131] Russia's proposals often highlight so-called gaps – areas where international law has not explicitly anticipated digital tools. For instance, Russia and China have pushed UN resolutions to elaborate new legal rules on sovereignty in cyberspace, seeking limits on illegal cross-border hacking and intelligence gathering.[132]

Russia's 2018–2020 initiatives vividly illustrate this approach. After disagreements in the UN Group of Experts, Russia successfully led the creation of an Open-Ended Working Group (at the UN) to negotiate a more inclusive treaty process. In UN forums, Russian delegates have repeatedly called for a legally binding instrument on information security. In their view, such a treaty would explicitly codify the interplay of sovereignty, non-intervention, and use of force in the cyber domain.[133] Western and

[127] Haataja (n 45).
[128] Robert Collett and Nayia Barmpaliou, '*International cyber capacity building: global trends and scenarios', European Union Institute for Security Studies*, September 2021..
[129] Schmitt and Pakkam (n 37).
[130] Sukumar and Basu (n 100).
[131] Elaine Korzak, '*Russia's Cyber Policy Efforts in the United Nations', North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence,* Tallinn Paper No 11, 2021, https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf, accessed 21 September 2025.
[132] Sukumar and Basu (n 100).
[133] Ibid.

North Atlantic Treaty Organization countries have generally opposed a new treaty in the First Committee, arguing instead for implementing voluntary norms. Russia counters that without a formal agreement, states will continue to flout rules and interpret them opportunistically. This divide reflects broader political splits: supporters of a treaty (Russia, China, some Global South countries) tend to emphasize state sovereignty and security, whereas most Western states warn that a rigid treaty could be used to justify censorship or constraints on the free internet.[134] Even though Russia now concedes international law's core validity, it insists a treaty is indispensable to fill current gaps and enhance cyber stability.[135]

6. Case Study – Cyber Intrusion on Critical Infrastructure

A. Scenario setup

Imagine a sudden, coordinated cyber-attack against critical infrastructure in the Black Sea–Eastern Mediterranean region. In this scenario, a malicious malware campaign (e.g. a modified industrial-control system virus) is launched against a nation's power grid and a major seaport's management systems. Within hours, the citylights in a capital go dark, hospitals lose backup power, and automated port cranes grind to a halt, halting grain exports. Emergency services struggle without communications. Computer forensics trace the operation to a sophisticated hacker unit using tools apparently aligned with a hostile state's military cyber-intelligence program, although attribution is delayed by layers of proxies. The scale of disruption is severe: it causes human harm (e.g. power failures endanger medical patients) and economic losses. Because this hypothetical attack is linked (directly or indirectly) to a state adversary and mimics the effects of conventional warfare, it raises the question: how would international law categorize it?

For context, real-world precedents underscore the stakes. In December 2015, Ukraine's power grid was similarly struck by malware, cutting electricity to hundreds of thousands. Analysts attributed that incident to a Russian unit called Sandworm. No

[134] Ibid.
[135] Korzak (n 130).

fatalities were reported, but the attack demonstrated how a cyber breach could paralyze civilian infrastructure.[136] In our scenario, we assume an even more disruptive campaign in the strategically sensitive Black Sea–Eastern Mediterranean (region) zone.

B. Legal characterization

Legally, a key question is whether this cyber-operation constitutes a use of force under UN Charter Article 2(4), and if so whether it rises to the level of an armed attack triggering the victim's Article 51 right of self-defense.[137] International law provides few bright-line rules for cyber cases, but several principles guide the analysis. First, any cyber act with force-like effects – physical damage, destruction, or casualties – potentially violates the force prohibition, even if carried out without guns or bombs.[138] For example, Tallinn Manual 2.0 (the international experts' guide) holds that a cyber operation causing real-world physical damage would qualify as a violation of sovereignty or non-intervention, and potentially as a use of force if intended to coerce or harm.[139]

States assess the effects and scale. Low-level intrusions (brief website defacements, data theft, minor service outages) are analogous to espionage or nuisance; they do not constitute a use of force in the Charter sense.[140] By contrast, an attack inflicting serious destruction – say, melting equipment or causing loss of life – would likely be deemed akin to a conventional attack.[141] In our scenario, because hospitals lost power and civilians faced danger, one could argue an armed attack occurred. The authoritative Tallinn Manual rules (though not legally binding) would support treating an extensive cyber blackout with life-threatening consequences as triggering self-defense.[142] Other factors include intent and context: if it is clear the assault was

[136] Congressional Research Service, '*Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience'*, CRS Report R48067, 17 May 2024, https://www.everycrsreport.com/files/2024-05-17_R48067_ec9b146372fac1c17e466dabba91199bfafbe564.html, accessed 21 September 2025.

[137] Schmitt (n 70).

[138] Haataja (n 45).

[139] Ibid.

[140] Schmitt and Pakkam (n 37).

[141] International Committee of the Red Cross (n 48).

[142] Ben Hines, 'Reinterpreting the Legality of Forcible Self-Defence in Response to Non-Kinetic Cyber Attacks' (2024) *Melbourne Journal of International Law, Vol.* 25 (1), 411-428, 414.

coordinated by a state actor with military objectives, this strengthens the armed-attack characterization.[143] Conversely, if damage were limited to data theft or temporary disruption without physical harms, some legal scholars might view it as unlawful interference short of armed aggression. The lack of casualties or purely economic impact, for example, has in past incidents kept them below the armed-attack threshold. Ultimately, the legal classification hinges on a holistic judgment: the level of impact (damage, human harm), the target's nature (critical civilian infrastructure), and the attribution.[144]

C. Policy response and implications

How would affected states respond? If the attack is judged an armed attack, the victim state (and its allies) could invoke collective self-defense under Article 51 of the UN Charter – including potentially North Atlantic Treaty Organization's Article 5.[145] North Atlantic Treaty Organization summits have affirmed that cyberattacks can count as Article 5 triggers depending on their severity.[146] In our scenario, if power outages were extensive and attributed to an adversary, the struck country might call an Article 4 consultation or even ask for collective action. North Atlantic Treaty Organization's 2016 Warsaw Summit declared cyberspace a new operational domain and reaffirmed that defense obligations apply to cyber operations.[147] Thus, serious Black Sea–Eastern Mediterranean (region) cyber aggression could, in theory, mobilize Alliance solidarity (possibly involving defensive cyber operations, sanctions, or even kinetic backup).

However, if decision-makers deem the effects below the armed-attack threshold, the incident may be treated as a criminal or law-enforcement matter. The victim might arrest (or indict) identifiable hackers, bolster cybersecurity patrols, and

[143] Eduardo Cavalcanti de Mello Filho, 'Armed Attacks against Merchant Vessels: "Looking behind the Flag" to Find the victim State' (2024) 29 *Journal of conflict & Security Law,* 281-309, 283.
[144] Eichensehr (n 117).
[145] François Delerue, 'The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack', in *Cyber Operations and International Law* (Cambridge: Cambridge University Press, 2020), ch 6, 273–342, 275.
[146] North Atlantic Treaty Organization, *Vilnius Summit Communiqué*, Press Release (2023) 001, 11 July 2023, https://www.North Atlantic Treaty Organization.int/cps/en/North Atlantic Treaty Organizationhq/official_texts_217320.htm, accessed 21 September 2025.
[147] Wiedemar (n 83).

appeal to international institutions (e.g. UN condemnation) rather than go to war.[148] Historically, states often prefer cyber responses such as naming-and-shaming, intelligence sharing, and targeted sanctions when evidence is inconclusive. For instance, in response to past hacks, Western states have imposed sanctions on hostile actors instead of military retaliation.[149]

The ambiguity of cyber attribution thus critically shapes the choice of response. If evidence finally confirms clear state sponsorship, the victim state might feel justified in a military counter-strike or collective defense – but only if political and legal thresholds are met. Otherwise, states are more likely to pursue proportional countermeasures (such as offensive cyber operations in self-defense) or diplomatic/legal recourse.[150] Even after something like the 2015 Ukraine blackout, the response was cyber resilience building and international pressure, not open warfare.[151] In our hypothetical, leaders would weigh the costs of escalation against the need to uphold norms: a visible cyber assault on people's lives certainly tests the line between a law-enforcement issue and an act of war. The choice of pathway – collective defense under North Atlantic Treaty Organization, or policing the incident – would ultimately depend on allies' judgment of the attack's gravity and the confidence of attribution. This analysis contends that maintaining strategic ambiguity regarding cyber thresholds is detrimental to regional stability. States must instead adopt 'declaratory deterrence,' explicitly defining the critical infrastructure attacks that will trigger collective defense.[152]

7. Bridging the Gap: Legal adaptations

[148] Finlay and Payne (n 8).

[149] Martha Finnemore and Duncan B Hollis, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity' (2020) 31 *European Unionropean Journal of International Law* 969, 976.

[150] W. C. Banks, 'The Bumpy Road to a Meaningful International Law of Cyber Attribution' (2019) 113 *AJIL Unbound* 191, 195.

[151] Eichensehr (n 117).

[152] F J Egloff and M Smeets, 'Publicly attributing cyber attacks: a framework' (2023) *Journal of Strategic Studies 46* 502–533, 514 https://doi.org/10.1080/01402390.2021.1895117

A. Clarifying Armed Attack in Cyberspace

Current law uses the Nicaragua scale and effects test (ICJ 1986) to identify an armed attack.[153] The paper proposes concretely defining digital analogues. For example, states could adopt objective thresholds akin to kinetic strikes: if a cyber operation inflicts physical destruction, casualties or major system failure, it counts as an armed attack. Several governments already suggest similar criteria. Germany's stance explicitly notes that indirect injury or death from a cyber-operation may count, and France regards considerable economic damage as a factor.[154] Likewise, widespread disruption of critical infrastructure (power grids, water systems, etc.) should be treated as the functional equivalent of a bombing run.[155] Conversely, low-level intrusions (even if politically sensitive) would remain below the threshold. In practice, a treaty or declaration might enumerate concrete indicators (e.g. fatalities, blackout >X hours, market losses >Y) to trigger Article 51 response.[156] Intent should also be weighed: operations deliberately designed to mimic the effects of conventional attacks should be treated identically, whereas cyber espionage or routine crime (the hacking of non-essential data for theft) would not.[157] By analogizing to physical armed attacks, states make clear that a cyber bomb (e.g. a virus that bursts a dam or crashes an airliner's systems) is as unlawful as any artillery shell.[158] Defining a digital armed-attack with objective benchmarks – scale (casualties, outages), effect (physical destruction), and hostile intent – would give governments a bright line for lawful self-defense.[159]

B. Applying Jus in Bello to Cyber

In an armed conflict, all cyber weapons and tactics must comply with established International Humanitarian Law (the law of armed conflict). This means cyber operations in war must respect distinction, proportionality, and precautions just

[153] Finlay and Payne (n 8).
[154] Schmitt and Pakkam (n 37).
[155] Haataja (n 45).
[156] Jakub Spáčil, 'Cyber Operations against Critical Financial Infrastructure: a Non-Destructive Armed Attack?' (2022) *International and Comparative Law Review,* Vol. *22* (2), 27–42, 28.
[157] Schmitt and Pakkam (n 37).
[158] Ibid.
[159] Ibid.

like bombs or bullets.[160] The International Committee of the Red Cross emphasizes that any cyber act reasonably expected to cause injury, death or physical damage is an attack subject to International Humanitarian Law.[161] Even non-physical assaults – for example a digital strike that shuts down hospital systems or contaminates water treatment controls – would qualify as attacks because they endanger civilians.[162] Accordingly, cyber weapons (malware, botnets, viruses, etc.) are not exempt. States should explicitly require that all new cyber capabilities undergo the same Article 36 review as conventional arms.[163] In target selection, commanders must distinguish between military and civilian cyber infrastructure: for instance, a missile guidance network (military objective) can be lawfully disrupted, but a civilian banking server cannot, even if attacked by code.[164] Likewise, measures of last resort are needed: war planners should avoid collateral data loss by, for example, freezing the malware if it drifts into non-military systems. The paper suggests codifying these principles by stating that all cyber means are means of warfare under International Humanitarian Law, triggering existing rules.[165] This might take the form of military manuals or international guidelines stating that (a) civilian networks and data are protected objects, (b) attackers must foresee and mitigate any incidental civilian harm, and (c) commanders must conduct weapon reviews for new cyber tools.[166] Strengthening these norms – as the Tallinn Manual has begun to do in its commentary – would close such loopholes. There is no cyber exception to the laws of war. Digital attacks must observe distinction and precaution just like any other weapon.[167]

C. Enhancing Attribution and State Responsibility

[160] International Committee of the Red Cross (n 48).

[161] International Committee of the Red Cross (n 35).

[162] B. Abbou and others, 'When all computers shut down: the clinical impact of a major cyber-attack on a general hospital' (2024) *Frontiers in Digital Health* 6 1321485.

[163] Natalia Jevglevskaja, 'Challenges to Article 36 Reviews Posed by (Autonomous) Cyber Capabilities', in *International Law and Weapons Review: Emerging Military Technology under the Law of Armed conflict* (Cambridge, Cambridge University Press 2021), 239–70, 244 0.

[164] Schmitt (n 54).

[165] International Committee of the Red Cross (n 48).

[166] Schmitt (n 54).

[167] International Committee of the Red Cross (n 48).

Cyber attackers often hide behind layers of anonymity or proxy actors. To address this issue, the paper recommends strengthening collective attribution mechanisms and clarifying how state responsibility is applied.[168] This could involve international protocols for joint investigation of major intrusions. For example, an independent multi-state panel (similar to the Organisation for the Prohibition of Chemical Weapons for chemical attacks) could examine high-profile incidents and publicly report findings.[169] At a minimum, victim and transit states should form rapid-response teams (e.g. joint Computer Security Incident Response Team/Computer Emergency Response Team task forces) to share forensic evidence on attacks.[170] The (UN) Group of Governmental Experts's Norm 27 already urges cooperation among national cybersecurity agencies and diplomats in incident analysis.[171] The paper further proposes that states make such cooperation routine. For instance, agreements to share malware signatures, network logs or threat intelligence across borders would greatly improve situational awareness and certainty.

Under the general rule of international law, a state is responsible in cyber conflicts if it knows or intends that malicious cyber actors (even private contractors or proxy militias) are operating from its territory.[172] This follows the principle that a state should not knowingly allow its territory to be used for wrongful acts. In other words, harboring or contracting out hacking-for-hire would violate a duty of due diligence.[173]

---

[168] Yuval Shany and Michael N Schmitt, 'An International Attribution Mechanism for Hostile Cyber Operations' (2020) 96 *International Law Studies* 196, 199.

[169] *François Delerue*, 'Reflections on the Opportunity of an International Attribution and Accountability Mechanism for Cyber Operations', *QIL QDI*, 31 July 2024, https://www.qil-qdi.org/reflections-on-the-opportunity-of-an-international-attribution-and-accountability-mechanism-for-cyber-operations/, accessed 21 September 2025.

[170] European Union Agency for Cybersecurity (ENISA), '*2020 Report on Computer Security Incident Response Team-LE Cooperation: A study of the roles and synergies among selected European Union Member States/EFTA countries', ENISA*, January 2021, https://www.enisa.EuropeanUnionropa.European Union/sites/default/files/publications/ENISA%20Report%20on%20Computer Security Incident Response Team-LE%20Cooperation%20-%20A%20study%20of%20the%20roles%20and%20synergies%20among%20selected%20countries.pdf, accessed 21 September 2025.

[171] UN Group of Governmental Experts Report on Responsible State Behaviour (n 65).

[172] Antonio Coco and Talita de Souza Dias, 'Cyber Due Diligence: A Patchwork of Protective Obligations in International Law' (2021) 32 *European Union Journal of International Law* 771, 776 https://doi.org/10.1093/ejil/chab056.

[173] Ibid.

On the other hand, a state that is merely the unwitting source of random malware (without knowledge) would not be held immediately responsible. Importantly, states must investigate and punish cybercrime within their borders.[174] This means enacting laws to prosecute cyber-attacks and enforcing them strictly – much like how states treat terrorism.[175] To make accountability credible, the paper encourages establishing that directing or controlling a proxy cyber militia is equivalent to state action.[176] An aggressor state cannot hide behind non-state hackers without consequence. Once attribution is confirmed, diplomatic and legal measures (such as sanctions or indictments) should be applied.[177]

D. Clarify Reporting and Transparency Obligations

Finally, the paper recommends new norms regarding reporting and openness to build mutual confidence. States should announce in advance which cyber actions would cross their red lines, such as attacks causing large-scale casualties or targeting specific critical systems. After an incident, they should promptly notify relevant parties – allied states, affected nations, or the UN – with technical details of what occurred.[178] The 2021 UN Group of Governmental Experts even recommends that a victim state formally notify the State from which the activity is emanating and seek cooperation in confirming the facts. Adopting such steps (even as voluntary guidelines) would reduce misunderstanding and rumor.[179] The paper suggests a model similar to arms-control transparency measures: timely incident reports and requests for clarifications (possibly via diplomatic hotlines or the existing Nuclear Risk Reduction Centers) should be standard practice. Over the longer term, coalitions of willing states could compile an annual overview of significant cyber incidents, analogous to the IAEA incident

[174] Ibid.

[175] Jennifer Trahan, 'The Criminalization of Cyber-Operations under the Rome Statute' (2021) *19 J Int'l Crim Just* 1133, 1138.

[176] Canfil (n 114).

[177] Chimène I Keitner, 'Attribution by indict ment' (2019) 113 *American Journal of International Law* 207–12, 208.

[178] UN Group of Governmental Experts Report on Responsible State Behaviour (n 65).

[179] Ibid.

reporting or UN arms reports.[180] Carving out expectations of notice and fact-sharing – rather than post-facto secrecy – would anchor cyberspace in greater accountability.[181]

8. Multilateral and Diplomatic Initiatives

A. UN Group of Governmental Experts and Open-Ended Working Group (at the UN) Processes

At the United Nations, two tracks – the UN Group of Governmental Experts and the Open-Ended Working Group – have become the primary forums for cyber norm-building.[182] The 2013–2015 (UN) Group of Governmental Experts and Open-Ended Working Group (at the UN) (2019–2021) explicitly affirmed that existing international law applies to cyberspace, producing lists of responsible-behavior norms.[183] These bodies rely heavily on case study–driven diplomacy. For instance, Australia submitted detailed hypothetical scenarios to show how the UN Charter and Geneva law govern cyber (e.g. cyber-attacks on hospitals or ports).[184] Numerous state non-papers contain fictional incidents to flesh out the rules. Importantly, the Open-Ended Working Group (at the UN) allows space for stakeholders: intersessional meetings often include technical experts, industry, Non-Governmental Organizations and academics.[185] The paper encourages continuing this practice: expert panels can

[180] Open, informal, cross-regional group of the Open-Ended Working Group (at the UN) Confidence Builders, '*Confidence-Building Measures – A recap and a vision for the future permanent mechanism*', *UN Office for Disarmament Affairs*, Joint Working Paper, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_%282021%29/Open-Ended Working Group (at the UN)_Confidence_Builders_Working_paper_on_CBMs_in_the_permanent_future_mechanism.pdf, accessed 21 September 2025.

[181] N. Tsagourias and F Middleton, 'Fact-Finding and Cyber Attribution' in R Buchan, D Franchini and N Tsagourias (eds), *The Changing Character of International Dispute Settlement: Challenges and Prospects* (Cambridge: Cambridge University Press, 2023) 439–66, 443.

[182] Nanette S Levinson, 'Idea entrepreneurs: The United Nations Open-Ended Working Group & cybersecurity' (2021) *Telecommunications Policy,* Vol. *45* (6), 102142.

[183] UN Group of Governmental Experts Report on Responsible State Behaviour (n 65).

[184] Department of Foreign Affairs and Trade (Australia), '*Australia Non Paper: Case studies on the application of international law in cyberspace',* Non-paper, DFAT, 2020, https://www.dfat.gov.au/sites/default/files/australias-Open-Ended Working Group (at the UN)-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf, accessed 21 September 2025.

[185] Levinson (n 181).

analyze model incidents (like election hacking or grid failures) and present them at UN forums. Through such concrete examples, states refine their positions.[186] The (UN) Group of Governmental Experts reports also proposed cooperative measures (like instructing states to notify each other of vulnerabilities) and recommended inviting bodies like the International Law Commission to study how law applies to cyber.[187] The UN processes serve as diplomatic laboratories: by discussing specific cases and negotiating voluntary norms (the 2015 (UN) Group of Governmental Experts's 11 norms, for instance), they gradually build a shared understanding of how the charter applies online.[188]

B. North Atlantic Treaty Organization/European Union and Regional Cooperation

Military and regional alliances are key venues for operationalizing cyber norms. North Atlantic Treaty Organization, for example, has long affirmed that a significant cyberattack could invoke Article 5 collective defense.[189] North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence (Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization)) even trains armed forces on legal scenarios.[190] Notably, the Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization) Cyber Law Toolkit and its legal exercises (like Locked Shields and Cyber Coalition) integrate jus ad bellum and jus in bello issues into war games, ensuring that national forces practice respecting international law.[191] North Atlantic Treaty Organization's recent summits (Wales 2014,

[186] Sheetal Kumar, 'The missing piece in human-centric approaches to cybernorms implementation: the role of civil society' (2021) *Journal of Cyber Policy,* Vol. 6 (3), 375–393, 379.
[187] UN Group of Governmental Experts Report on Responsible State Behaviour (n 65).
[188] Levinson (n 181).
[189] Finlay and Payne (n 8).
[190] North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization), *Training Catalogue, 2024* (Updated 10 September 2024), https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/uploads/2024/09/2024_North Atlantic Treaty Organization_CCD_COE_Training_Catalogue_final_revSept2024.pdf, accessed 21 September 2025.
[191] North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, 'Cyber Law Toolkit 2024', 2023, https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/news/2023/cyber-law-toolkit/, accessed 21 September 2025.

Warsaw 2016) have formally recognized cyberspace as an operational domain and committed Allies to strengthen network resilience.[192]

The European Union also supports joint cyber resilience in the Black Sea–Eastern Mediterranean region. The European Union's new Black Sea Security Strategy explicitly commits to building capacity, cooperation and information sharing on hybrid and cyber threats among regional partners.[193] It calls for using CSDP missions, European Union technical assistance and coordination with North Atlantic Treaty Organization to protect critical infrastructure. This could involve joint exercises (for example, drills simulating power-grid attacks with allied navies participating), shared cyber defense training, and coordinated public warnings when a wave of digital attacks is detected.[194] For instance, the European Union and North Atlantic Treaty Organization have launched structured dialogues on cybersecurity, and European Union programs now fund cyber defense capacity-building in Eastern Mediterranean countries.[195] These multilateral activities should reinforce the norms identified in UN fora, by familiarizing Black Sea/East Mediterranean militaries and technocrats with the same legal standards (e.g. rules for targeting, incident reporting).

C. Multi-Stakeholder Diplomacy

Creating norms should not be left to governments alone. Achieving broad support requires engaging industry, academia and civil society. Prominent industry accords have already begun this work: for instance, the Microsoft-led Cybersecurity Tech Accord and the Siemens Charter of Trust set voluntary standards (banning data ransom,

[192] Mikkel Storm Jensen, 'Five good reasons for North Atlantic Treaty Organization's pragmatic approach to offensive cyberspace operations' (2022) 22 *Defence Studies* 464, 466.
[193] European Unionropean Commission and High Representative of the Union for Foreign Affairs and Security Policy (n 90).
[194] Annegret Bendiek and Mika Kerttunen, '*Enhancing European Union-North Atlantic Treaty Organization Cooperation in Preparedness and Critical Infrastructure Protection',* SWP Working Paper No 06, June 2025, https://www.swp-berlin.org/publications/products/arbeitspapiere/SWP_WP_Enhancing_European_Union-North_Atlantic Treaty Organization_Cooperation_Critical_Infrastructure_Protection_Bendiek_Kerttunen.pdf, accessed 21 September 2025.
[195] European Union CyberNet, '*Mapping of European Union-funded External Cyber Capacity Building Actions 2022',* European Unionropean Commission, 2023, https://www.European Unioncybernet.European Union/wp-content/uploads/2023/04/mapping-report-on-European Union-funded-external-cyber-capacity-building-actions-2022.pdf, accessed 21 September 2025.

protecting medical and election systems, etc.).[196] Likewise, the 2018 Paris Call for Trust and Security in Cyberspace is a multi-stakeholder pledge (endorsed by 70+ states, 1500 companies and Non-Governmental Organizations) around nine principles – including protecting individuals and critical infrastructure from cyberattack.[197] Such initiatives amplify legal norms by translating them into industry practice and public expectation. The paper suggests that official diplomacy regularly seek input from these constituencies. For example, UN Open-Ended Working Group (at the UN) sessions have benefited from civil society briefings, and North Atlantic Treaty Organization encourages expert academia to advise on rule nuances.[198] Standards bodies also play a role. International technology standards (such as ITU guidelines or ISO protocols) can incorporate legal requirements for precautions and resilience.[199] By including private-sector experts and Non-Governmental Organizations, states can use technical know-how and moral influence. A rule, for example, prohibiting cyberattacks on hospitals will have more impact if hospital networks and software vendors also commit to defending against such exploits.[200] Organizing regular public–private roundtables or issuing joint codes of conduct (as some digital coalitions have done) can unite legal norms with practical measures. For example, the Paris Call demonstrates this approach. It involves broad participation from governments, industry and Non-Governmental Organizations, giving many parts of society a stake in upholding these norms (for

[196] Roxana Radu, Matthias C Kettemann, Trisha Meyer and Jamal Shahin, 'Normfare: Norm entrepreneurship in internet governance' (2021) *Telecommunications Policy,* Vol. *45* (6), 102148.

[197] Kaja Ciglic and John Hering, 'A Multi-Stakeholder Foundation for Peace in Cyberspace' (2021) *Journal of Cyber Policy 6,* 360–374, 366.

[198] Ian Johnstone, Arun Sukumar and Joel Trachtman, 'Building cybersecurity through multistakeholder diplomacy: Politics, processes, and prospects' in Ian Johnstone, Arun Sukumar and Joel Trachtman (eds), *Building an International Cybersecurity Regime: Multistakeholder Diplomacy* (Edward Elgar Publishing, 2023).

[199] Irene Kamara, 'European Unionropean cybersecurity standardisation: A tale of two solitudes in view of European Unionrope's cyber resilience' (2024) *Innovation: The European Union Journal of Social Science Research* 1–20, 11..

[200] Priya Urs, Talita Dias, Antonio Coco and Dapo Akande, '*The International Law Protections against Cyber Operations Targeting the Healthcare Sector', Oxford Institute for Ethics, Law and Armed conflict*, University of Oxford, April 2023, https://www.elac.ox.ac.uk/wp-content/uploads/2023/04/ELAC-Research-Report_International-Law-Protections-against-Cyber-Operations-Targeting-the-Healthcare-Sector.pdf, accessed 21 September 2025.

example, tech companies learn to secure their software and media organizations learn to flag propaganda).[201]

D. Confidence-Building Measures

Finally, states should negotiate confidence-building measures to reduce cyber tensions. Historical analogies are instructive; during the Cold War, hotlines and incident-reporting agreements helped prevent escalation.[202] A similar toolkit can be adapted for cyberspace. For instance, quick channels for sharing information between adversaries can defuse crises. The 2013 U.S.-Russia cyber pact is a good example; it established direct contacts between US-Computer Emergency Response Team and its Russian counterpart to exchange threat indicators in real time.[203] It also repurposed the old US–Russia nuclear hotline (the Nuclear Risk Reduction Center) to allow formal inquiries about suspected cyberattacks, and even set up a secure voice line between Washington and Moscow for cyber incidents.[204] The paper recommends extending such ideas to North Atlantic Treaty Organization/European Union networks – for instance, establishing a regional incident-warning hotline linking Black Sea countries' Computer Emergency Response Teams. Other specific CBMs include: conducting joint cyber exercises (e.g. simulating cross-border attacks while respecting no-fire lines), pre-notification of major exercises to avoid misidentification, and sharing anonymized data on threats. On deterrence, Allied states could publicly affirm that a massive cyber attack on a North Atlantic Treaty Organization or European Union member would activate collective defense (echoing Article 5), thereby raising the costs for potential aggressors.[205] Confidence-building means range from practical tech collaboration

[201] Ciglic and Hering (n 196).

[202] Paul Meyer, 'Confidence-building measures in cyberspace' in Eneken Tikk and Mika Kerttunen (eds), *Routledge Handbook of International Cybersecurity* (Routledge 2020).

[203] Lora Saalman, Fei Su and Larisa Saveleva Dovgal, '*Cyber Risk Reduction in China, Russia, the United States and the European Union', Stockholm International Peace Research Institute (SIPRI)*, June 2024, https://www.sipri.org/sites/default/files/2024-06/cyber_risk_reduction.pdf, accessed 21 August 2025.

[204] Rose Gottemoeller and Daniil Zhukov, *'Nuclear Risk Reduction Centers: A Stable Channel in Unstable Times', Stanley Center for Peace and Security*, October 2023, https://stanleycenter.org/wp-content/uploads/2023/10/Nuclear-Risk-Reduction-Centers-Gottemoeller-Zhukov.pdf ,(accessed 21 August 2025.

[205] OSCE, '*10 Years of OSCE Cyber/Information and Communications Technology Security Confidence-Building Measures',* OSCE Secretariat, 2023)https://www.osce.org/files/f/documents/f/7/555999_1.pdf, accessed 21 August 2025.

(information sharing, shared Computer Emergency Response Team platforms) to diplomatic commitments (joint statements or sanctions pledges for violations). By baking these measures into alliances, the region can deter rash cyber aggression and mitigate accidents before they spiral.[206]

9. Implications for Regional Stability and Conclusion

A. Reinforcing Rule of Law

Clarifying the application of universal international law to regional threats ultimately strengthens the rules-based security architecture in the Black Sea–Eastern Mediterranean nexus. When states clearly define the conditions for self-defense and the obligations during conflict, unpredictability decreases.[207] Applying existing international law to cyberspace provides a victim state with a "tool kit" to identify violations, assign responsibility, resolve disputes peacefully or take lawful countermeasures. A well-defined legal framework makes state behavior more predictable and reduces the risk of uncontrolled escalation. If governments agree in advance on what counts as a legal or illegal cyber act, responses become deliberate instead of knee-jerk.[208] This predictability supports justice – victims see that wrongdoing is addressed through the law (sanctions, indictments, collective defense) rather than through revenge or a power vacuum. A transparent legal regime (with adapted jus ad bellum and jus in bello principles) also helps vulnerable states resist coercion, as they can point to shared rules when defending their actions. Over time, internalizing these norms will help treat cyberspace aggression as a regulated domain, not an anarchic Wild West.[209] Closing the legal gaps reaffirms the system of laws that

[206] Robert Collett, 'Understanding cybersecurity capacity building and its relationship to norms and confidence building measures' (2021) *Journal of Cyber Policy,* Vol. 6(3) 298–317, 302.

[207] Russell Buchan, 'Non-forcible measures and the law of self-defence' (2023) *International & Comparative Law Quarterly,* Vol. *72* (1) 1–33.

[208] United Nations General Assembly, '*Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States'*, UN Doc A/76/136, 28 May 2021, https://digitallibrary.un.org/record/3933543/files/A_76_136-EN.pdf, accessed 21 August 2025.

[209] Gisel, Rodenhauser and Dörmann (n 56).

all parties have pledged to follow, reinforcing a rules-based order amid constant digital threats.,*B. Maintaining Social and Political Cohesion*

For people in the region, strong cyber norms would increase trust in institutions and reduce public panic during cyber incidents. If citizens see their governments responding to a cyber crisis with established legal measures – for example, notifying allies, providing clear explanations and sanctioning the perpetrators – confidence remains intact. This also prevents rumors or panic that might otherwise spread after mysterious outages or disinformation campaigns.[210] Moreover, by involving diverse stakeholders (governments, tech companies, civil society) in building these norms, the public sees cyber defense as a collective effort rather than a secret arms race.[211] For instance, the Paris Call demonstrates this. It has broad participation from governments, industry and Non-Governmental Organizations, giving many parts of society a stake in upholding these norms (for example, tech companies commit to secure their software and media organizations learn to flag propaganda).[212] Consequently, when an incident occurs, multiple trusted voices can promote a coherent, lawful response rather than discord. In practical terms, clear cyber rules help authorities quickly classify an event (as a crime, not war) and respond appropriately, avoiding overreaction that can frighten populations.[213] Thus, reinforcing international norms in cyberspace directly supports social cohesion – citizens of Black Sea/East Med states will be less likely to feel abandoned or vulnerable if they know a legal playbook governs their defense.[214]

C. Summary of Recommendations

[210] R. Shandler and M. A. Gomez, 'The hidden threat of cyber-attacks – undermining public confidence in government' (2023) *20 Journal of Information Technology & Politics* 359, 365.

[211] K. Ciglic and J. Hering, 'A multi-stakeholder foundation for peace in cyberspace' (2021) *Journal of Cyber Policy,* Vol. *6* (3), 360–374.

[212] Arun Sukumar, Dennis Broeders and Monica Kello, 'The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy,' (2024) *Contemporary Security Policy,* Vol. 45 (1), 7.

[213] ENISA, '*Best Practices for Cyber Crisis Management,'* February 2024, https://www.enisa.European Unionropa.European Union/sites/default/files/2024-11/ENISA%20Study%20Best%20Practices%20Cyber%20Crisis%20Management.pdf, accessed 21 September 2025.

[214] Sabanadze and Dalay (n 20).

In conclusion, bridging the cyber gap in the Black Sea–Eastern Mediterranean requires both legal adaptation and cooperative diplomacy. Legally, states must refine jus ad bellum by explicitly defining what a cyber armed attack means (for instance, catastrophic physical effects) and clarifying the thresholds for self-defense. They must also integrate jus in bello into cyber by affirming that digital operations obey all International Humanitarian Law rules (distinction, proportionality, and Article 36 weapon reviews). In parallel, responsibility and transparency are vital: international mechanisms should be strengthened so that attribution of cyber incidents is credible (through joint investigations and evidence-sharing), and states should agree to cooperative reporting (notification of attacks and red-lines) to prevent misperception. Diplomatically, Non-Governmental Organization's multilateral forums (the UN Group of Governmental Experts and Open-Ended Working Group) must continue unpacking these norms through case-study discussions. Regional and alliance structures (North Atlantic Treaty Organization, the European Union, Black Sea security initiatives) should incorporate these norms into exercises, training and policy (for example, by simulating cyber incidents in military drills and issuing joint statements on cyber defense). Crucially, these efforts should engage all stakeholders: governments should invite the private sector, technical experts and civil society into norm-building (as in the Paris Call and industry accords), since broad adherence to the rules enhances stability. Confidence-building measures – from Computer Emergency Response Team information-sharing to incident hotlines – will further deter reckless behavior. By combining clear legal rules with robust international collaboration, the cyber gap in the Black Sea–Eastern Mediterranean can be closed, thus preventing the erosion of international order and preserving both security and societal cohesion in the region.

Bibliography

Abbou B and others, ‘When all computers shut down: the clinical impact of a major cyber-attack on a general hospital’ (2024) 6 Frontiers in Digital Health 1321485

Abraham D, Houmb SH and Erdodi L, ‘Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation’ (2025) 15 Applied Sciences 9233

Akyeşilmen N, 'Türkiye in the Global Cybersecurity Arena: Strategies in Theory and Practice' (2022) 24(3) Insight Turkey 109

Androjna A and others, 'Assessing Cyber Challenges of Maritime Navigation' (2020) 8 J Mar Sci Eng 776

Atlantic Council Task Force on Black Sea Security, *A Security Strategy for the Black Sea* (Atlantic Council 2023)

Axt H-J, 'Conflicts and Global Powers in the Eastern Mediterranean. An Introduction' (2022) 70 Comparative Southeast European Studies 393

Banks WC, 'The Bumpy Road to a Meaningful International Law of Cyber Attribution' (2019) 113 AJIL Unbound 191

Bendiek A and Kerttunen M, *Enhancing EU-NATO Cooperation in Preparedness and Critical Infrastructure Protection* (SWP Working Paper No 06, 2025)

Bendiek A, Bund J and Kerttunen M, 'The Attribution Dividend: Protecting Critical Infrastructure from Cyber Attacks' (SWP Comment 2024/C 46, 2024)

Bradshaw S, Bailey H and Howard PN, *Industrialized Disinformation: 2020 Global Inventory of Organised Social Media Manipulation* (Oxford Internet Institute 2021)

Broeders D, 'Private active cyber defense and (international) cyber security—pushing the line?' (2021) 7 Journal of Cybersecurity tyab010

Buchan R, 'Non-forcible measures and the law of self-defence' (2023) 72(1) International & Comparative Law Quarterly 1

Bueger C and Liebetrau T, 'Critical Maritime Infrastructure Protection: What's the Trouble?' (2023) 155 Marine Policy 105772

Burton J and Stevens T, 'System, Alliance, Domain: A Three-Frame Analysis of NATO's Contribution to Cyber Stability' in Chesney R (ed), *Cyberspace and Instability* (Edinburgh University Press 2022)

C4ADS, *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria* (C4ADS 2019)

Canfil JK, 'The Illogic of Plausible Deniability: Why Proxy Conflict in Cyberspace May No Longer Pay' (2022) 8 Journal of Cybersecurity tyac007

Cavalcanti de Mello Filho E, 'Armed Attacks against Merchant Vessels: "Looking behind the Flag" to Find the Victim State' (2024) 29 Journal of Conflict & Security Law 281

Centre for Strategic and International Studies, 'Navigating Security Challenges in the Black Sea Region' (CSIS 2024)

Ciglic K and Hering J, 'A Multi-Stakeholder Foundation for Peace in Cyberspace' (2021) 6(3) Journal of Cyber Policy 360

Clavijo Mesa MV, Patino-Rodriguez CE and Guevara Carazas FJ, 'Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains' (2024) 15 Information 710

Coco A and de Souza Dias T, '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law' (2021) 32 European Journal of International Law 771

Collett R, 'Understanding cybersecurity capacity building and its relationship to norms and confidence building measures' (2021) 6(3) Journal of Cyber Policy 298

Collett R and Barmpaliou N, *International cyber capacity building: global trends and scenarios* (European Union Institute for Security Studies 2021)

Congressional Research Service, *Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience* (CRS Report R48067, 2024)

Council of the European Union, 'Cyberspace: Council approves declaration on a common understanding of application of international law to cyberspace' (Press release, 18 November 2024)

Council of the European Union, *Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace* (ST-15833-2024-INIT, 2024)

Decree of the President of Ukraine No 447/2021, *On the Cybersecurity Strategy of Ukraine* (National Security and Defense Council of Ukraine 2021)

Delerue F, *Cyber Operations and International Law* (Cambridge University Press 2020)

Delerue F, 'Reflections on the Opportunity of an International Attribution and Accountability Mechanism for Cyber Operations' (2024) QIL QDI

Delerue F, 'The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack' in *Cyber Operations and International Law* (Cambridge University Press 2020)

Department of Foreign Affairs and Trade (Australia), *Australia Non Paper: Case studies on the application of international law in cyberspace* (DFAT 2020)

Dickson J and Harding E, 'How a Cyber Alliance Took Down Russian Cybercrime' (Center for Strategic and International Studies 2025)

Eaton T, 'Self-Defense to Cyber Force: Combatting the Notion of "Scale And Effect"' (2021) 36 American University International Law Review 697

Egloff FJ, 'Public attribution of cyber intrusions' (2020) 6 Cybersecurity tyaa012

Egloff FJ and Smeets M, 'Publicly attributing cyber attacks: a framework' (2023) 46 Journal of Strategic Studies 502

Eichensehr KE, 'Ukraine, Cyberattacks, and the Lessons for International Law' (2022) 116 American Journal of International Law 145

ENISA, *Best Practices for Cyber Crisis Management* (2024)

Ertan A and others (eds), *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* (NATO CCDCOE Publications 2020)

EU CyberNet, *Mapping of EU-funded External Cyber Capacity Building Actions 2022* (European Commission 2023)

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *The European Union's strategic approach to the Black Sea region* (JOIN(2025) 135 final, 2025)

European Union Agency for Cybersecurity, *2020 Report on CSIRT-LE Cooperation: A study of the roles and synergies among selected EU Member States/EFTA countries* (ENISA 2021)

Finlay L and Payne C, 'The Attribution Problem and Cyber Armed Attacks' (2019) 113 AJIL Unbound 202

Finnemore M and Hollis DB, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity' (2020) 31 European Journal of International Law 969

FP Analytics, *Digital Front Lines* (FP Analytics 2023)

Gisel L, Rodenhäuser T and Dörmann K, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' (2020) 102 International Review of the Red Cross 287

Gorwa R and Peez A, 'Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord' in Broeders D and van den Berg B (eds), *Governing Cyberspace: Behaviour, Power and Diplomacy* (Rowman & Littlefield 2020)

Gottemoeller R and Zhukov D, *Nuclear Risk Reduction Centers: A Stable Channel in Unstable Times* (Stanley Center for Peace and Security 2023)

Haataja S, 'Cyber operations against critical infrastructure under norms of responsible state behaviour and international law' (2023) 30 International Journal of Law and Information Technology 423

Halisdemir E, *National Cybersecurity Organisation: TURKEY* (NATO Cooperative Cyber Defence Centre of Excellence 2021)

Hines B, 'Reinterpreting the Legality of Forcible Self-Defence in Response to Non-Kinetic Cyber Attacks' (2024) 25(1) Melbourne Journal of International Law 1

International Committee of the Red Cross, *International humanitarian law and cyber operations during armed conflicts* (Position paper, 2019)

International Committee of the Red Cross, 'International humanitarian law and cyber operations during armed conflicts' (2020) 102 International Review of the Red Cross 481

International Institute for Strategic Studies, *Cyber Capabilities and National Power: A Net Assessment* (Research Paper, 2021)

Jensen B, Valeriano B and Whitt S, 'How cyber operations can reduce escalation pressures: Evidence from an experimental wargame study' (2024) 61 Journal of Peace Research 119

Jensen MS, 'Five good reasons for NATO's pragmatic approach to offensive cyberspace operations' (2022) 22 Defence Studies 464

Jevglevskaja N, 'Challenges to Article 36 Reviews Posed by (Autonomous) Cyber Capabilities' in *International Law and Weapons Review: Emerging Military Technology under the Law of Armed Conflict* (Cambridge University Press 2021)

Jiang Z, 'Regulating the Use and Conduct of Cyber Operations through International Law: Challenges and Fact-finding Body Proposal' (2020) 5 LSE Law Review 59

Jiguet F and others, 'GNSS spoofing in conflict zones disrupts wildlife tracking and hampers research and conservation efforts' (2025) 16 Nat Commun 1199

Johnstone I, Sukumar A and Trachtman J, 'Building cybersecurity through multistakeholder diplomacy: Politics, processes, and prospects' in Johnstone I, Sukumar A and Trachtman J (eds), *Building an International Cybersecurity Regime: Multistakeholder Diplomacy* (Edward Elgar Publishing 2023)

Kajander A, *Unnecessary Repetition: Russia's Latest Attempt at a New UN Convention on Cyberspace* (NATO Cooperative Cyber Defence Centre of Excellence 2023)

Kamara I, 'European cybersecurity standardisation: A tale of two solitudes in view of Europe's cyber resilience' (2024) Innovation: The European Journal of Social Science Research 1

Katagiri N, 'Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks' (2021) 7 Journal of Cybersecurity tyab009

Keitner CI, 'Attribution by Indictment' (2019) 113 American Journal of International Law 207

Kello L, 'Cyber legalism: why it fails and what to do about it' (2021) 7(1) Journal of Cybersecurity tyab014

Korzak E, *Russia's Cyber Policy Efforts in the United Nations* (Tallinn Paper No 11, NATO Cooperative Cyber Defence Centre of Excellence 2021)

Kumar S, 'The missing piece in human-centric approaches to cybernorms implementation: the role of civil society' (2021) 6(3) Journal of Cyber Policy 375

Lațici T, *Understanding the EU's approach to cyber diplomacy and cyber defence* (European Parliamentary Research Service 2020)

Levinson NS, 'Idea Entrepreneurs: The United Nations Open-Ended Working Group & Cybersecurity' (2021) 45 Telecommunications Policy 102142

Lu C and others, 'Overview of satellite nav spoofing and anti-spoofing techniques' (2024) 12 Frontiers in Physics 1428544

Lysenko A and Gunitsky S, 'The invisible front: Ukraine's IT army and the evolution of cyber resistance' (2025) 41 Post-Soviet Affairs 263

Mačák K, 'Unblurring the lines: military cyber operations and international law' (2021) 6 Journal of Cyber Policy 411

Meyer P, 'Confidence-building measures in cyberspace' in Tikk E and Kerttunen M (eds), *Routledge Handbook of International Cybersecurity* (Routledge 2020)

Mickonytė A, 'Obligation to Mutual Assistance Under Article 42(7) TEU: The Conundrum of Intentional Ambiguity' (2024) 18 ICL Journal 311

Moynihan H, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention* (Chatham House Research Paper, 2019)

Moynihan H, 'The vital role of international law in the framework for responsible state behaviour in cyberspace' (2021) 6(3) Journal of Cyber Policy 394

NATO Cooperative Cyber Defence Centre of Excellence, *Cyber Law Toolkit 2024* (2023)

NATO Cooperative Cyber Defence Centre of Excellence, *Training Catalogue, 2024* (2024)

NATO, *Cyber defence* (2024)

NATO, *Hybrid threats and hybrid warfare* (2024)

NATO, 'Vilnius Summit Communiqué' (Press Release (2023) 001, 2023)

Nijs M, 'Humanizing siege warfare: Applying the principle of proportionality to sieges' (2020) 102(914) International Review of the Red Cross 683

Oorsprong F, Ducheine P and Pijpers P, 'Cyber-attacks and the right of self-defense: a case study of the Netherlands' (2023) 6 Policy Design and Practice 217

Open informal cross-regional group of the OEWG Confidence Builders, *Confidence-Building Measures – A recap and a vision for the future permanent mechanism* (Joint Working Paper, UN Office for Disarmament Affairs)

Ormrod A, Ormrod D and Slay J, 'Cyber Offensive Operations in Hybrid Warfare: Observations from the Russo-Ukrainian Conflict' (2023) 22(1) Journal of Information Warfare 76

OSCE, *10 Years of OSCE Cyber/ICT Security Confidence-Building Measures* (OSCE Secretariat 2023)

Pomson O, 'Methodology of identifying customary international law applicable to cyber activities' (2023) 36 Leiden Journal of International Law 1023

Praks H, *Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage* (Hybrid CoE Working Paper 32, European Centre of Excellence for Countering Hybrid Threats 2024)

Prucková M, *Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO* (NATO Cooperative Cyber Defence Centre of Excellence 2021)

Radu R and others, 'Normfare: Norm entrepreneurship in internet governance' (2021) 45(6) Telecommunications Policy 102148

Reinhold T, Pleil H and Reuter C, 'Challenges for Cyber Arms Control: A Qualitative Expert Interview Study' (2023) 16 Zeitschrift für Außen- und Sicherheitspolitik 289

Roguski P, 'An Inspection Regime for Cyber Weapons: A Challenge Too Far?' (2021) 115 American Journal of International Law Unbound 111

Romanosky S and Boudreaux B, 'Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government' (2020) 34 International Journal of Intelligence and CounterIntelligence 463

Ryan S, 'Submarine Communication Cables and Belligerent Rights in Armed Conflict' (2024) 38 Ocean Yearbook 459

Saalman L, Su F and Dovgal LS, *Cyber Risk Reduction in China, Russia, the United States and the European Union* (Stockholm International Peace Research Institute 2024)

Sabanadze N and Dalay G, *Threat Perceptions and the Failure of Signalling in Understanding Russia's Black Sea Strategy: How to Strengthen Europe and NATO's Approach to the Region* (Chatham House Research Paper, 2025)

Schmoldt J, 'Cyber proxies: covert state–non-state interactions in cyberwarfare' in Stevens T and Devanny J (eds), *Research Handbook on Cyberwarfare* (Edward Elgar Publishing 2024)

Schmitt MN, 'Cyber Symposium – The Evolution of Cyber Jus ad Bellum Thresholds' (Lieber Institute for Law and Warfare 2022)

Schmitt MN, 'Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace' (2020) 3 Texas National Security Review 32

Schmitt MN, 'Wired warfare 3.0: Protecting the civilian population during cyber operations' (2019) 101 International Review of the Red Cross 333

Schmitt MN and Pakkam AS, 'Cyberspace and the Jus ad Bellum: The State of Play' (2024) 103 International Law Studies 194

Shandler R and Gomez MA, 'The hidden threat of cyber-attacks – undermining public confidence in government' (2023) 20 Journal of Information Technology & Politics 359

Shany Y and Schmitt MN, 'An International Attribution Mechanism for Hostile Cyber Operations' (2020) 96 International Law Studies 196

Sherman J, 'Unpacking Russia's cyber nesting doll' (Atlantic Council 2025)

Sherman J, *Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior* (Atlantic Council 2022)

Spáčil J, 'Cyber Operations against Critical Financial Infrastructure: a Non-Destructive Armed Attack?' (2022) 22(2) International and Comparative Law Review 27

Sukumar A and Basu A, 'Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order' (2024) 9(2) Journal of Cyber Policy 256

Sukumar A, Broeders D and Kello M, 'The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy' (2024) 45 Contemporary Security Policy 7

The White House, *National Cybersecurity Strategy* (2023)

Todorov Y, 'Navigating Uncharted Waters: Tackling Maritime Cybersecurity Challenges in the Black Sea Region' (2024) 55(2) Information & Security: An International Journal 113

Trahan J, 'The Criminalization of Cyber-Operations under the Rome Statute' (2021) 19 J Int'l Crim Just 1133

Triandafyllidou A and Monteiro S, 'Migration narratives on social media: Digital racism and subversive migrant subjectivities' (2024) 29(8) First Monday

Tsagourias N and Middleton F, 'Fact-Finding and Cyber Attribution' in Buchan R, Franchini D and Tsagourias N (eds), *The Changing Character of International Dispute Settlement: Challenges and Prospects* (Cambridge University Press 2023)

UN General Assembly, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States* (A/76/136, 2021)

UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (A/76/135, 2021)

UN Security Council, *Record of the open debate on Maintenance of international peace and security: cybersecurity* (S/2021/621, 2021)

Urs P and others, *The International Law Protections against Cyber Operations Targeting the Healthcare Sector* (Oxford Institute for Ethics, Law and Armed Conflict 2023)

US Department of Health & Human Services Health Sector Cybersecurity Coordination Center, *Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector* (HC3, 2023)

Wiedemar S, *NATO and Article 5 in Cyberspace* (CSS Analyses in Security Policy No 323, Center for Security Studies 2023)

Zabierek L and others, *US-Russian Contention in Cyberspace* (Belfer Center for Science and International Affairs 2021)