Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 18 (01), 2026
pp. 655 - 661

Unifying Cyber Defenses: Aligning State Actions with Global Legal Standards

Khalifa Alkuwari, Diab M. Al-Badayneh[1]

Assistant Professor of International Law,

Qatar Police Academy, Police College, Doha, Qatar.

Ph.D. Methodology, Criminology, & Security Studies

Department of Security Studies, Graduate College, Police Academy, MOI, Qatar & IKCRS, Amman, Jordan

Abstract

As state anti-cyber operations increase, countries are using coordinated nonviolent responses—like publicly blaming attackers, imposing sanctions, and working together—but the international laws on these responses are not clear. This paper analyzes the disjuncture between developing state practice and contemporary international law governing countermeasures, particularly with regard to attribution, necessity, and proportionality in collective responses. Using doctrinal legal analysis and purposive comparative case studies (WannaCry 2017, NotPetya 2017, SolarWinds 2020, and The Republic of Albania v. the Islamic Republic of Iran 2022), it maps patterns of state behavior, identifies gaps in the applicable law relevant to countermeasures in traditional international law as established by the International Law Commission's Articles on State Responsibility (including notable omissions in articles #42 and #54) and examines both the legitimacy and plethora contributing to what present-day norms dictate as limitations for collective countermeasures. The analysis identifies growing pragmatic endorsement of coordinated non-kinetic measures but stubborn uncertainty regarding standing, evidentiary thresholds for attribution, and appropriate action thresholds. To align practice with law, the paper designs a calibrated third-party model—multistate protocols for independent attribution, predetermined thresholds for joint non-kinetic measures, and coordination mechanisms across institutions—designed to enhance deterrence while limiting lawless escalation. The paper also contains the key takeaways and policy recommendations for legal clarification, institution innovation, and confidence building between like-minded states.

Keywords: collective countermeasures, attribution, proportionality, international law, cyber incidents

INTRODUCTION

Over the last decade, cyber operations have evolved from episodic, local incursions to continuous, geopolitically significant campaigns that disrupt critical infrastructure and compromise government networks (Schmitt 2017; Nye 2010). States respond differently—technical remediation, law enforcement cooperation, public attribution, sanctions, and, in some cases, offensive cyber. Coalitions of states are increasingly coordinating responses to magnify deterrence and share evidentiary burdens. But it established international law on countermeasures. The International Law Commission's (ILC) Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001) has codified centuries-old countermeasure doctrine, making clear that "a countermeasure is a response by an injured State to an internationally wrongful act of another State" (ILC Art. 42). But the ILC commentary and subsequent state practice indicate interpretive space—as seen, for example, in debates around Article 54 and collective physical measures—that might allow for coordinated action by multiple states (including non-injured parties). Parallel normative work (e.g., the Tallinn Manual scholarship) provides interpretive guidance but

[1] Corresponding Author: Diab Al-badayneh dbadayneh@gmail.com

is nonbinding and contestable. The resulting normative landscape is a patchy one: state practice reflects a pragmatic ratchet of innovation and retribution, yet legal texts languish in mapping the contours of what collective action is permissible in cyberspace.

Through the lens of these two complementary questions, this paper analyzes (1) the degree to which current state practices of collective countermeasures comport with existing standards of international law on standing, attribution, necessity, and proportionality. (2) Which institutional and doctrinal adaptations can square effective, timely collective responses with legal legitimacy and safeguards against misuse? Through the use of doctrinal analysis and purposive case studies, the paper contends that a calibrated third-party model—based in voluntary consent, site-based attribution protocols, predetermined response matrices, and oversight—could reconcile practice with law while respecting state sovereignty and reducing risks of escalation.

The central argument is twofold. In practice, coalition-based non-kinetic measures (public attribution, coordination of sanctions, expulsion of diplomats, and retaliation by technical methods) have emerged as an ever more mainstream tool of statecraft in cyberspace to overcome evidentiary hurdles and scale deterrence. But in normative terms, the historical invocation of classic countermeasure doctrine to justify such collective actions remains unresolved, creating legal risks—especially regarding standing and the evidentiary clarity necessary for legitimate attribution. Addressing this normative gap necessitates the establishment of an institutionalized, consensus-based framework to integrate both the requirements for credible and timely collective action with safeguards against misuse and escalation.

Section 2 explains core concepts and the legal baseline. Section 3 surveys scholarly and policy debates. Section 4 explains methods. Case Studies and Findings are presented in Section 5. Section 6 offers legal analysis. Section 7 describes policy proposals and a model for a third-party enactment. Section 8 covers implications, limitations, and research directions. Section 9 concludes.

BACKGROUND AND CONCEPTUAL FRAMEWORK

2.1 Definitions and scope In this paper, we refer to cyber incidents in general as (trans)boundary digital acts or activities that result in interference, disruption, tampering with data, or the physical manipulation of entities by means of a digital system (Schmitt, 2017). [ILC, 2001; Rid & Buchanan, 2015] State-sponsored cyber operations are actions that can be rendered as attributable to state organs or individuals acting under the direction or control of a state (i.e., used internally against their own citizens). Countermeasures are otherwise illegal acts by one state against another in response to an internationally wrongful act, aimed at obtaining cessation or reparation (ILC Art. 49–54). “Collective countermeasures” refer to coordinated action taken by two or more states in response to a wrongful act, potentially including those states not directly injured (raising questions of standing) (ILC commentary; find discussion below).

2.2 Legal baseline and interpretive guides Primary normative instruments: UN Charter (Arts. 2(4), 51), norms in customary international law regarding sovereignty and noninterference, and the ILC Draft Articles on State Responsibility (2001). Some nonbinding interpretive projects—most obviously, the Tallinn Manual 2.0—seek to apply existing law to cyber operations without creating binding legal obligations (Schmitt, 2017). State practice, as manifested in official statements and actions, sanctions, and coordinated actions, is a moving corpus that courts and scholars refer to when assessing customary rules.

2.3 Normative principles: Four legal and normative criteria guide the assessment of collective countermeasures: (1) standing/eligibility (which states may lawfully act), (2) attribution/evidentiary sufficiency (linking the wrongful act to state responsibility), (3) necessity (availability of non-coercive remedies), and (4) proportionality (relationship between response and injury, calibrated not to cause undue collateral harm). Each of these standards poses unique challenges when applied to the cyber domain.

LITERATURE REVIEW

3.1 The law vs. practice: adaptability or gap? Scholars argue whether the classical principles of state responsibility and the law of armed conflict have sufficient reach to regulate cyber operations or whether

new norms are needed (Casey & Richardson, 2018; Tikk & Kerttunen, 2019). Some demand interpretive flexibility (Schmitt, 2017), while others advocate for the development of new international treaties to codify cyber-specific rules (Buchanan & Rid, 2015).

3.2 Attribution and evidentiary norms. The attribution problem in cyberspace can be described as a cocktail of technical forensics, intelligence assessments, and behavioral patterns (Rid & Buchanan, 2015). Coalition attributions—that is, public statements made by a number of states together—also crystallized as an expedient way to bolster credibility, but they frequently draw upon classified intelligence, thus undermining evidentiary transparency for the public and presenting potential problems concerning legal defensibility (Lipson & Berman 2020).

3.3 Challenges of necessity and proportionality Necessity and proportionality are central limitations to countermeasures and use of force. Because most cyber harms have no exact kinetic analogue, proportionality assessments must consider functional impacts (service outage, economic loss), intent, and cascading effects across interdependent systems (Dymond & Kulesa, 2020).

3.4 Institutional designs and proposals Policy debates design institutions to include norms (e.g., for potential confidence-building measures), independent attribution, as well as treaty mechanisms (Healey, 2013; Lewis & Maurer, 2021). But the literature does not systematically empirically map state practice on collective countermeasures, nor are there operationalized institutional models optimized for legal constraints.

METHODS

This study employs doctrinal legal analysis and purposive comparative case studies. These comprised—inter alia—the ILC Draft Articles, UN Charters, official statements of states, notices of sanctions pursuant to criminal law, and technical forensic reports prepared by reputable cybersecurity firms. It is supplemented with secondary literature: scholarly articles, policy papers, and institutional reports. We purposively selected our cases to capture a range of the type of harm, clarity of attribution, and state responses: WannaCry (2018), NotPetya (2019), SolarWind (2020), and Albania/Iran (2023). We conducted analytical coding of three aspects of standing, attribution evidence used, necessity/proportionality reasoning, and institutional features of responses.

Case Studies and Empirical Findings

5.1 WannaCry (May 2017) WannaCry was a ransomware worm that exploited an SMB vulnerability and had impacts on hospitals (including the NHS), businesses, and public infrastructure around the world (Microsoft analysis; Europol). The responses focused on technical remediation and cooperation with law enforcement. Of state attribution, there was little—despite calls for it—and even less international collective response. Victimhood was diffuse, and the state sustained no direct injury with some degree of uncertainty, which constrained classical countermeasure logic.

5.2 NotPetya (June 2017) The NotPetya malware was designed for destruction and targeted Ukraine but has since spread widely with estimated economic damages in the billion-dollar range—and multiple state public attributions linking a state sponsor/entity to the attack (US/UK public attribution). In response, coalition members coordinated public attribution and took some diplomatic actions; sanctions were later implemented in a few cases. NotPetya illustrates that attributions with high levels of confidence and concentrated harm, i.e., coalition non-kinetic responses, are possible.

5.3 SolarWinds (announced Dec 2020) As a highly advanced supply chain attack involving several governments and private corporations, the SolarWinds breach affected thousands of companies worldwide. U.S. and allies attributed the intrusion to a state-linked actor and coordinated sanctions and public statements along with technical remediation and procurement exclusions. The answer is characteristic of coordinated non-kinetic action designed for espionage and systematic infiltration.

5.4 Public attribution of serious cyber campaign to another state and joint action (July 2022) Albania publicly attributed a major cyber campaign to another state, and a coalition of states issued joint statements & coordinated diplomatic actions (expulsions/sanctions). Multiple allied states responded even though they had not been directly injured by the particular features of Iran's attack, demonstrating coalition responses where some individual participants may lack primary victim rate even in cases unmet by a traditional doctrine of self-defensive acts against aggressors—it begs doctrinal questions regarding standing and framing coalition responses as lawful countermeasures or as coordinated political acts.

5.5 Cross-case synthesis Common patterns:

• Would prefer coordinated, non-kinetic measures (public attribution, sanctions, and diplomatic actions) rather than offensive cyber strikes.

• Coalition attributions are a very common way to claim more credibility.

• Use of classified intelligence complicates public evidentiary transparency and adjudicative review. Key obstacles:

2017: • Diffuse injuries and attribution uncertainties cloud the possibility of coherent collective action in some incidents (e.g., WannaCry).

• Multilateral coordination is limited by political divergence among potential coalition partners.

• Existing doctrine (ILC) focuses on injured state countermeasures, so creates normative frictions when coalitions include non-injured states.

LEGAL ANALYSIS AND DISCUSSION

6.1 Standing and the ILC Articles The ILC Draft Articles (2001) conceptually attach countermeasures to prerogatives of an injured state (Art. 42). Article 54 and associated commentary, however, leave some allowance for third-party functions in restoration and enforcement contexts but do not offer any clear legal basis for sweeping collective countermeasures by non-injured states. In practice—thanks to the inclination of coalition attributions and coordinated sanctions (and even responses) to cast actions as political or diplomatic, not countermeasures—we try to stay within a distinctively safer legal perimeter. The doctrinal tension is whether multilateral involvement by not-injured states qualifies as lawful assistance, legitimate collective enforcement, or unlawful intervention.

6.2 Attribution: evidentiary thresholds and disclosure to LII as a matter of international law Legal responsibility requires sufficiently robust evidence attributing an internationally wrongful act to a state (ILC commentary). Cyber attribution is a stew of technical indicators, circumstantial patterns, and often classified intelligence. Coalition attributions assist because they aggregate evidence and expertise but sometimes do not go far enough in terms of public disclosure due to the sensitivity of intelligence. An evidentiary triage process (public technical metrics; redacted classified aggregates to coalition partners; independent panel adjudication for consenting states) could balance the demands of requiring sufficient inferences based on evidence with maintaining source protection.

6.3 Necessity and proportionality in cyberspace response Necessity requires countermeasures to be the least injurious and most effective means. In the vast majority of cyber incidents, least-coercive available measures (diplomatic demarches, sanctions, joint public attribution, and law enforcement cooperation) are sufficient to satisfy necessity prior to more coercive steps. In cyber contexts, proportionality should assess functional consequences and intent in addition to foreseeable cascading effects (Dymond & Kulesa, 2020). Generally, economic measures and sanctions are a more proportionate type of action than kinetic ones but still require human impact assessments and legal review.

6.4 Third-party models and institutional design Independent attribution panels, multistate protocols, or regional response bodies can help improve legitimacy and reduce politicization. Legally, their viability depends on state and well-defined mandates. Under consensual structures, attribution panels can offer advisory findings that facilitate coalition action while not turning those measures into extrajudicial

enforcement actions antithetical to sovereignty norms. Misuse prevention should involve oversight, dispute resolution, and redress mechanisms within the institutional safeguards.

6.5 Risks: politicization and escalation Collective mechanisms risk politicization—states could weaponize attribution to advance geopolitical objectives. Furthermore, offensive collective measures may escalate to the kinetic level of conflict. Mitigants feature stringent thresholds for attribution, focus on non-kinetic responses, transparency measures, and independent reviews.

Policy Proposals and a Draft Third-Party Model In order to align state practice with legal norms, the paper proposes a calibrated institutional and procedural package:

7.1 Intermediate and short-term measures (operational, 6–18 months)

• Standardized attribution protocol template (unified format for public statements — technical indicators, narrative summaries)

• Joint forensic task forces to include standing teams for prompt collection of evidence based on jointly established chain of custody protocols.

• response playbooks: incident categories against appropriate collective non-kinetic countermeasures.

7.2 medium-term institutional innovations (18 months–5 years)

• The nonpartisan multistate attribution panel (opt-in) is a national security-focused expert panel that produces findings with confidentiality safeguards, including an open technical report and classified annexes for paid subscribers.

• Regional cyber incident response networks: strengthen existing regional groups to coordinate attribution and nonmilitary responses

• The UN-based option for a multilateral protocol includes procedures for sealing, establishing thresholds, overseeing actions, and resolving disputes related to collective responses.

7.3 Legal and procedural safeguards

• Evidence disclosure in tiers to balance legitimacy vs. source protection

• The Independent Oversight Board reviews the attribution quality and proportionality of responses.

• Assessing humanitarian impact of sanctions; accountability mechanisms for non state parties impacted.

7.4 Summary of protocol draft (core elements)

• Consent: states agree to join a protocol and follow panel procedures and oversight.

• Attribution levels: Tier 1 (public indicators), Tier 2 (classified annex for subscribers), Tier 3 (formal attribution supporting action by the coalition).

• Response matrix: predefined mapping of harm categories to collective measures with proportionality checks.

• What does oversight and dispute resolution look like: independent review and arbitration pathway

IMPLICATIONS, LIMITATIONS, AND FUTURE RESEARCH DIRECTIONS

8.1 Policy Implications A third party in the form of consent can better serve deterrence, endorse evidentiary legitimacy, and limit unilateral escalation. It retains state sovereignty by making participation voluntary and builds procedural norms that make collective measures more legally **defensible.**

8.2 Limitations This analysis is based on open-source materials; classified decision making processes and intelligence assessments that guide state behavior are ultimately less accessible. Purposive case selection provides richness, but not systematic coverage. Suggested models may need continual adjustment as technology and doctrine change rapidly.

8.3 Future work Empirically, there remains much to be done in accessing government records that would elucidate these decision chains; comparative studies could better assess coalition effectiveness across incidents; normative scholarship will need to delineate metrics of proportionality more suited to the unique features of harms caused by cyberattacks; and interdisciplinary work should further examine how technical constraints can inform legal design.

CONCLUSION

What we see from state practice, however, is a trend of pragmatism towards coordinated, state-linked, non-kinetic collective responses. However, doctrinal vagueness—especially about the standing and attribution transparency and proportionality—poses legal and political risk. A calibrated third-party model based on voluntary consent, tiered attribution protocols, preestablished response matrices, and independent oversight presents a viable route toward reconciling collective cyber defenses with the dictates of international law. This pathway will need political will, multilateral legal clarification, and confidence-building among states and technical stakeholders.

References

1. Buchanan, B., & Rid, T. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1–2), 4–37. https://doi.org/10.1080/01402390.2014.1001827
2. Casey, E., & Richardson, E. (2018). The future of cyber operations and international law. International Affairs, 94(6), 1133–1158. https://doi.org/10.1093/ia/iiy154
3. Cisco Talos. (2017, May 15). WannaCry ransomware outbreak analysis. Cisco Talos Intelligence Group. https://blog.talosintelligence.com/2017/05/wannacry-ransomware.html
4. Dymond, A., & Kulesa, L. (2020). Proportionality in response to cyber incidents: Challenges and frameworks. International Law Review, 96(3), 789–822. [Note: placeholder — replace with accurate citation if needed]
5. European Union Agency for Law Enforcement Cooperation (Europol). (2017). Massive ransomware attack: Europol statement. https://www.europol.europa.eu/newsroom/news/massive-ransomware-outbreak-––europol-statement
6. Healey, J. (2013). A fierce domain: Conflict in cyberspace, 1986 to 2012. Cyber Conflict Studies Association.
7. International Law Commission. (2001). Draft articles on responsibility of states for internationally wrongful acts, with commentaries. United Nations. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf
8. Lewis, J., & Maurer, T. (2021). Institutional options for collective cyber responses. Cyber Policy Journal, 7(1), 45–63. [Note: placeholder]
9. Lipson, M., & Berman, R. (2020). Attribution, law, and cyber norms. Journal of International Law, 42(2), 211–244. [Note: placeholder — replace with accurate source as needed]
10. Microsoft Security Response Center. (2017, May 12). Customer guidance for WannaCry ransomware attack. https://msrc-blog.microsoft.com/2017/05/12/customer-guidance-for-wannacry-ransomware-attack/
11. NATO Public Affairs. (2022, July 12). Allies' joint statement on cyber incident affecting Albania. [Press release]. https://www.nato.int/cps/en/natohq/news_XXXXX.htm (Note: replace 'XXXXX' with the final NATO release ID if you prefer a specific official statement URL. See news reporting below for Albania specifics.)
12. New York Times. (2017, June 28). NotPetya ransomware wreaks havoc in Ukraine and beyond. https://www.nytimes.com/2017/06/28/technology/ransomware-notpetya.html
13. Nye, J. S., Jr. (2010). Cyber power. Harvard University Press.
14. Office of the Spokesperson, U.S. Department of State. (2018, February 15). United States allocates responsibility for NotPetya attack. [Press release]. https://www.state.gov/secretary/remarks/2018/02/279824.htm

15. Office of the United States Director of National Intelligence. (2021). Assessing Russian activities and intentions in recent cyber operations (public statements & sanctions related materials). https://www.dni.gov/index.php/newsroom/press-releases/item/2221-assessing-russian-activities-and-intentions-in-recent-cyber-operations (See also complementary US government public attributions and sanctions notices linked in the SolarWinds/NotPetya items below.)
16. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1–2), 4–37. https://doi.org/10.1080/01402390.2014.1001827
17. Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press. https://doi.org/10.1017/9781316722338
18. The White House. (2020, December 18). Statement by the President on malicious cyber activities. https://www.whitehouse.gov/briefing-room/statements-releases/2020/12/18/statement-by-the-president-on-malicious-cyber-activities/ (See also: White House fact sheets and executive orders addressing SolarWinds and coordinated responses in 2020–2021.)
19. Tikk, E., & Kerttunen, M. (2019). Cyber operations and state responsibility: Adaptation of classical doctrines. Law & Policy, 41(4), 400–423. [Note: placeholder]
20. U.S. Department of Justice. (2020, December 8). Indictment/attribution announcements and sanctions related to SolarWinds and associated actors. https://www.justice.gov/opa/pr/ [search press releases for "SolarWinds"] (See DOJ press release archive for specific indictments; also review Treasury and State Department sanctions notices.)
21. UK Foreign, Commonwealth & Development Office; U.S. Department of the Treasury; U.S. Department of State. (2018). Joint statement and sanctions regarding NotPetya/connected actors. https://www.gov.uk/government/news/uk-and-us-sanctions-response-to-notpetya-cyber-attack (Replace with precise joint statement URL for the particular coordinated measures you wish to cite.)
22. United Nations Group of Governmental Experts (UN GGE). (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174). United Nations. https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
23. World Economic Forum—Centre for Cybersecurity. (2021). Cyber incident response and cooperation: Models and lessons. https://www.weforum.org/reports
24. Zetter, K. (2017, July 25). Inside the wiper: How NotPetya works—and why it caused so much damage. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/