Collective Countermeasures in Cyberspace: Bridging the Gap Between State Practice and International Legal Frameworks

Khalifa Alkuwari[1]

[1]Assistant Professor of International Law, Qatar Police Academy, Police College, Doha, Qatar.

Email: ka4090@pa.edu.qa - ORCID: https://orcid.org/0009-0008-9762-3605

Abstract: Cyberattacks are increasingly state-sponsored, as are the responses to them. However, existing frameworks do not adequately address the legalities of collective responses to state-sponsored cyberattacks. Although Article 42 of the International Law Commission's (ILC) Articles on State Responsibility (ASR) limits the right to take countermeasures to states that have been directly injured by cyber-attacks, the "savings clause" in Article 54 seems to contemplate collective action by non-injured states in response to erga omnes, meaning breaches of obligations owed to the international community as a whole. This article examines the legality and practicality of collective responses to cyberattacks, analyzing the tension between the traditional bilateral approach and the emerging advocacy for coordinated multilateral responses to cyber threats. Applying a doctrinal legal methodology, the article critically examines recent state practices, including the coordinated international response to the 2022 Iranian cyber-attack on Albania, the collective attribution of blame WannaCry (2017) and NotPetya (2017), and the European Union's Cyber Diplomacy Toolbox. The analysis explores the growing, but inconsistent, body of state practice and opinio juris, with notable divergences among those states that, like Estonia, explicitly endorse collective countermeasures, and those that , like France, reject them outright. The article also examines the substantive and procedural precedents to lawful countermeasures, such as attribution, proportionality, necessity, and the protection of third-party rights, and suggests how these conditions can address the special problems of operating in cyberspace. The article concludes by observing that, although the current legal framework does not explicitly authorize collective countermeasures, evolving state practices and the unique nature of cybersecurity are gradually making collective countermeasures more universally acceptable. The article concludes by proposing that the use of cyber countermeasures by third parties, if grounded in the theory of third-party coercion, could provide a legally sound rationale for collective responses that are effective deterrents, and respect both state sovereignty and the international rule of law...

Keywords: Collective Countermeasures; Cyberspace; State Responsibility; International Law; Cyber Operations

Introduction

The digital evolution of international relations may have irrevocably and fundamentally altered the very nature of interstate conflict. States are increasingly challenging the established norms of behavior in cyberspace on issues ranging from simple espionage and intellectual property theft to the widespread disruption of critical infrastructure and digital interference in democratic processes. Both the frequency and scale of State-sponsored cyber-operations have grown dramatically. Incidents such as the 2017 WannaCry ransomware attack, the 2017 NotPetya campaign, and the SolarWinds supply chain compromise of 2020, have caused significant transnational harm (Schmitt, 2017; Schmitt & Watts, 2021). Put simply, widespread harm resulting from state-sponsored cyber-operations is no longer merely hypothetical, but a bitter reality.

In response to these escalating threats, the international community has responded collectively: with states coordinating their efforts in cyberspace to attribute harm, to condemn the aggressor, and to

respond collectively to malicious cyber operations. Notable examples include the joint attribution of the WannaCry attack to North Korea by the United States, the United Kingdom, and numerous other states; the coordinated response of NATO allies and the European Union to Iran's 2022 cyber-attack on Albania; and the establishment of the European Union's Cyber Diplomacy Toolbox as a framework for collective diplomatic responses to cyber threats (Council of the European Union, 2017). These developments suggest the evolving practice of collective actions in cyberspace may be outpacing the legal frameworks designed to control them.

Historically, countermeasures in international law have been limited to bilateral measures: limiting the use of countermeasures to only the injured state, and their use limited to only inducing compliance only by the state responsible for an internationally wrongful act. The International Law Commission's Articles on State Responsibility (ASR) codify this understanding, with Article 42 restricting the right to take

countermeasures to the states directly injured and imposing strict conditions of proportionality, necessity, and reversibility (ILC, 2001; Crawford, 2013). However, the ASR are also ambiguous, in that Article 54, the so-called "savings clause," expressly reserves the question of whether non-injured states, acting in "the collective interest," may take "lawful measures" against a responsible state (ILC, 2001).

The ambiguity in the Articles on State Responsibility has produced a vigorous scholarly debate. Those favoring collective countermeasures assert that enforcement of global norms among increasingly interconnected global systems, particularly in cyberspace, requires a collective approach and should enable states beyond those directly injured to respond proportionately to serious breaches of international law (Dawidowicz, 2016; Tams, 2005). Others, on the other hand, fear that allowing non-injured states to take countermeasures risks abuse, disruption of interstate relations, and lacks sufficient support in both state practice and *opinio juris* to be recognized as customary international law (Focarelli, 2016).

This article seeks to bridge the divide between practice and doctrine by examining the evolving intersection between the doctrine of collective countermeasures and state practice in cyberspace. To do so, the article has three goals: map the legal framework governing countermeasures and the debate over collective action; second, analyze emerging state practice in collective cyber responses to assess its consistency with existing legal principles; and third, propose a practical reconceptualization of third-party cyber countermeasures that can both accommodate the realities of the digital age consistent with international law.

To do these things, the article takes a doctrinal approach to the law: systematically analyzing primary legal sources (including the ASR, ICJ jurisprudence, state position papers on international law in cyberspace, and Tallinn Manual 2.0), scholarly literature, and relevant state practices. Section 2 creates a conceptual framework by examining the foundations for collective countermeasures in international law; Section 3 collects, and analyses, emerging state practices in collective cyber responses; Section 4 addresses attribution, proportionality, and third-party rights, key legal challenges posed by collective cyber responses; Section 5 proposes a way to bridge the gap between practice and law; and Section 6 concludes the analysis and offers ideas for future research.

Conceptual Framework: Collective Countermeasures Under International Law

2.1 The Traditional Bilateral Paradigm

The law of countermeasures, as codified in Articles 49–54 of the ASR, is fundamentally bilateral. Article 49(1) defines "countermeasures" as measures taken by *an* "injured State" against *the* "responsible State" to induce compliance with the latter's obligations of cessation and reparation. Article 42 defines the "injured state" as (1) *the* state whose individual rights have been infringed; (2) which is uniquely affected by the breach of a collective obligation; or (3) as to which the breach radically alters the position

of all other states to which the obligation is owed (ILC, 2001). This construction reflects the well-established concept of state responsibility as a bilateral relationship between one wrongdoer and one victim.

It is well-established that countermeasures can be directed only (1) at the responsible state (Article 49(1)), only (2) temporarily and, as far as possible, (3) must be reversible (Article 49(3)). Countermeasures also must be proportionate to the injury suffered, considering the gravity of the internationally wrongful act and the rights in question (Article 51). To be lawful, countermeasures cannot affect fundamental obligations, including the prohibition of the use of force, the obligation to protect fundamental human rights, humanitarian obligations, nor violate diplomatic and consular agents (Article 50). Procedurally, the injured state must first demand that the responsible state fulfil its obligations under international law and warn it, in advance, of its decision to take countermeasures (Article 52) (ILC, 2001; Crawford, 2013).

2.2 The Emergence of Collective Countermeasures

One of the most contentious questions in the law of state responsibility is whether countermeasures are available to only the injured state. Article 48 of the ASR recognizes that states, other than the injured state, may assume the undisputed right of the injured state to take countermeasures, if the injured state is one of the group of states to which the obligation is owed, and the obligation protects the group's collective interest (*erga omnes partes* obligations), or if the obligation is owed to the international community as a whole (*erga omnes* obligations). However, Article 48 explicitly entitles non-injured states to only demand cessation and reparation; it does not expressly authorize them to take countermeasures against the responsible state (ILC, 2001).

This gap in Article 48, between the rights of injured states and the rights of non-injured states, is addressed—or, more accurately, deliberately left unresolved—by Article 54, which provides that the chapter on countermeasures "does not prejudice the right of any State, entitled under Article 48, paragraph 1, to invoke the responsibility of another State, to take lawful measures against that State to ensure cessation of the breach and reparation in the interest of the injured State or of the beneficiaries of the obligation breached." The ILC Commentary explains that this savings clause was adopted because the Commission could not agree on whether non-injured states could take countermeasures, while also recognizing that the practice was then "embryonic," but not wishing to foreclose its future development (ILC, 2001, Commentary to Article 54, para. 3). The article uses the term "lawful measures," rather than "countermeasures," "so as not to prejudice any position concerning measures taken in the general or collective interest" (ILC, 2001, Commentary to Article 54, para. 7).

Scholars are deeply divided on the legality of collective countermeasures. A significant body of scholarship supports their legality. Dawidowicz (2016) argues that a consensus is forming on the right of third-parties to take countermeasures as a matter of customary international law, on the basis that the international community of states as a whole has a legal interest in the performance of obligations *erga omnes*, supported by a substantial body of state practice since the 1970s. Similarly, Tams (2005) contends that the *erga omnes* obligations are enforceable only if non-injured states are permitted, if not encouraged, to take countermeasures. Similarly, Sicilianos (2010) and Alland (2002) argue that if collective countermeasures are banned, *erga omnes* obligations will be unenforceable. More recently, Al-Kuwari (2025) has also concluded that the right to collective countermeasures must be confined to responses to breaches of *erga omnes* obligations, precisely to prevent states from appointing themselves as enforcers of international law in cases in which they have no legal interest.

On the other side of the debate, Focarelli (2016)'s rigorous critique argues that existing state practices are insufficient to establish the rights of third-parties to take countermeasures as an international norm, but that recognizing such a right both carries significant risks of abuse by powerful states and, potentially, undermines the collective security regime of the UN Charter. He contends that much of the conduct cited as evidence of collective countermeasures can be characterized instead as retorsion—acts that, while unfriendly, are not themselves contrary to international law and therefore need not be justified under the doctrine of countermeasures (ILC, 2001; Crawford, 2013). This distinction is particularly significant in the domain of cyberspace, where the line between lawful and

unlawful responses is often unclear.

2.3 Countermeasures in the Cyber Domain

Applying the doctrine of countermeasures to cyberspace raises unique challenges that transcend the debate between bilateral and collective action. The Tallinn Manual 2.0, the most authoritative—though non-binding—application of international law to cyber operations, affirms that countermeasures are available in response to internationally wrongful cyber operations (Schmitt, 2017, Rule 20). The International Group of Experts has agreed that countermeasures may take cyber or non-cyber form, meaning that a state may respond to wrongful cyber operations through physical countermeasures, just as a state may respond to a wrongful physical intrusion with countermeasures in cyberspace (Schmitt, 2017, Rule 21).

However, the experts could not reach consensus on the question of collective countermeasures in cyberspace. This disagreement mirrors the broader divide between the theories espoused by scholars and the realities of state practice. Crucially, Rule 24 of the Tallinn Manual 2.0 provides that "only an injured State may engage in countermeasures, whether cyber in nature or not," a formulation that captures the current state of treaty law and is itself the central point of contention in the debate over collective countermeasures (Schmitt, 2017, Rule 24). Al-Kuwari (2025) has characterized this impasse as part of the broader debate between the 'bilateral approach' as embedded in the ASR and the 'collectivist approach' that scholars increasingly advocate and that is an emerging state practice, ultimately concluding that the collectivist approach is 'more aligned with the intent and purpose of the countermeasures rule,' given the unique characteristics of cyberspace.

Those states that have taken a position on the role of international law in cyberspace have adopted varying positions. Estonia, for example, has explicitly endorsed collective countermeasures in its national positions on international law in cyberspace (Estonia, Ministry of Foreign Affairs, 2019). The Netherlands has expressed support for collective countermeasures, though the precise conditions articulated in its position paper do not explicitly invoke Article 48 ASR by name, and Schmitt (2019) has observed that the Dutch letter notably makes no mention of collective countermeasures in its discussion of the conditions for lawful responses. At the other extreme, France has explicitly rejected collective countermeasures as a matter of principle, while accepting bilateral countermeasures in response to wrongful cyber operations (France, Ministère des Armées, 2019). Ireland has adopted a more nuanced position, accepting that collective countermeasures are permissible in limited circumstances, such as in response to violations of peremptory norms, but stopping short of endorsing a general right of collective countermeasures (Ireland, Department of Foreign Affairs, 2023, para. 26).

The characteristics of cyberspace intensify the arguments both for and against collective countermeasures. On one hand, the speed, scale, and interconnected nature of cyber operations mean that attacks frequently have effects that cross national boundaries, injuring multiple states simultaneously and creating a strong case for taking practical collective responses. On the other hand, the challenges of attribution in cyberspace—including the ease with which origins can be concealed, the use of proxy actors, and the ready availability of "false flag" techniques—create heightened risks of collective responses that are directed in error or are politically motivated. There is yet no consensus among states on whether collective countermeasures should be permitted in cyberspace (Schmitt, 2019), with many states preferring to frame their positions in ways that make no commitment to a specific legal framework, opting instead for strategic ambiguity, which Deeks (2020) labels "Defend Forward" operations.

State Practice and Emerging Trends in Collective Cyber Responses

3.1 Collective Attribution as a Precursor to Collective Countermeasures

The emergence of collective attribution, defined as coordinated public statements by multiple states that identify the perpetrator of a cyber operation may be the most significant development in collective cyber responses. Although attribution differs from countermeasures, the practice of collective attribution creates a political and evidentiary foundation for the justification of collective countermeasures.

The collective attribution of the WannaCry ransomware attack to North Korea in December 2017 was a watershed moment. The United States issued the initial attribution, which was promptly supported by the United Kingdom, Australia, Canada, New Zealand, Japan, and Denmark, among others. This coordinated response established a precedent for states acting in concert to publicly name the perpetrator of a major cyber operation. Similarly, the collective attribution of the NotPetya attack to Russia in February 2018 involved a coordinated effort by the United States, the United Kingdom, Australia, Canada, New Zealand, and several European states. These episodes demonstrated that collective action in the cyber domain was not merely theoretical but was becoming an established pattern of state practice (Efrony & Shany, 2018; Al-Kuwari, 2025). Al-Kuwari further notes that the NotPetya response—including coordinated economic sanctions against Russian entities—could be considered collective countermeasures if it were implemented collectively, as collective countermeasures involve actions that typically violate international trade obligations, but are justified as a collective response to an internationally wrongful act.

The significance of collective attribution extends beyond its immediate political effects. First, it contributes to the development of *opinio juris* regarding the legality of collective responses to cyber operations. When states coordinate their attributions, they are implicitly asserting a collective interest in cybersecurity and, potentially, in the right to respond collectively. This is particularly relevant if customary international law norms are to support collective countermeasures. The ILC has emphasized that "customary law" requires evidence of both general practice and the belief that such practice is required or permitted by law (ILC, 2018, Conclusion 2).

3.2 The Albanian Case

The 2022 Iranian cyber-attack on Albania is a pivotal point in the evolution of collective cyber responses. In July 2022, Iran launched a destructive cyber-attack against Albania, disrupting public services and destroying government data. Albania's investigation of the attack, supported by technical evidence from private cybersecurity firms and intelligence shared by allies, publicly attributed the attack to Iran in September 2022. Albanian Prime Minister Edi Rama responded by severing diplomatic relations with Iran, reportedly the first time a country has severed diplomatic ties in response to a cyber-attack (Rama, 2022).

Although the international response primarily demonstrated only political solidarity, rather than formal legal steps against Iran, it was notably collective in nature. For example, the North Atlantic Council publicly condemned the attack in the strongest possible terms, and expressed support for its affected ally (NATO, 2022). The United States deployed a "Hunt Forward" team through its Cyber Command to assist Albania bilaterally. Several individual NATO member states issued their own statements of condemnation. The European Union used its Cyber Diplomacy Toolbox framework to coordinate its members' statements by its members of diplomatic solidarity with Albania, and the United States, the United Kingdom, and numerous other states independently condemned Iran's actions. (CISA, Advisory AA22-264A, 2022).

The Albanian case is legally significant for several reasons. First, it demonstrated that the international community will treat seriously cyber-attacks on a state's civil infrastructure as violations of sovereignty and of the principle of non-intervention severe enough to merit collective responses. Second, it also illustrated that collective cyber responses could be practical, through multiple institutional channels: bilateral (the U.S. Hunt Forward deployment), regional (NATO's political solidarity), and supranational (the EU's coordinated diplomatic response). Third, it revealed the limitations of existing legal frameworks: despite broad consensus that Iran was responsible, no state explicitly characterized its response as a "collective countermeasure," and the legal justification for the coordinated responses remained deliberately ambiguous. Therefore, the states' responses were framed as demonstrating simple political solidarity and condemnation, rather than as enforcement measures under the law of state responsibility. Schmitt (2019) has observed this pattern in the broader context of collective cyber responses, noting that because there is yet no specific consensus on the permissibility of collective countermeasures, states will naturally, and acting in their own interests, avoid committing to specific legal positions on their legality.

3.3 The EU Cyber Diplomacy Toolbox

The European Union's Cyber Diplomacy Toolbox, created in 2017, is still the most robust institutional framework for collective cyber responses by a regional organization. The Toolbox provides a framework for proportionate diplomatic responses—such as restrictive measures (sanctions)—that the EU can deploy in response to malicious cyber activities, carefully calibrated to the scope, scale, duration, intensity, complexity, sophistication, and impact of the malicious activity (Council of the European Union, 2017; Council Decision (CFSP) 2019/797, Recital 4). Al-Kuwari (2025) has argued that if EU practice informs cybersecurity strategies in the GCC region, it is both because EU practices are clearly concerned with international legal obligations, and because the EU and the GCC have already developed various forms of inter-regional cooperation, including the 2022 elevation of the EU-GCC relationship to a 'Strategic Partnership.'

The EU activated its cyber sanctions regime for the first time in July 2020, targeting entities and individuals associated with cyber operations attributed to China, Russia, and North Korea, pursuant to Council Decision (CFSP) 2019/797. The Council's decision represented a significant collective cyber responses by a regional organization. The legal characterization of these sanctions has been challenged: although the EU has framed them as "autonomous restrictive" measures, rather than as countermeasures, Poli and Sommario (2023) emphasize the EU's deliberate failure to assign state responsibility to these measures, writing that "the adoption of [these] measures does not involve attribution of international responsibility for cyber-attacks to a third State" (Poli & Sommario, 2023). This deliberate legal restraint is itself analytically significant, because it suggests that the EU is deliberately avoiding characterizing its actions as countermeasures, which would require satisfying the conditions in Articles 49–54 ASR.

This ambiguity, significant because it was deliberate, is also legally significant. If the EU's cyber sanctions were actual countermeasures, they would support the use of collective countermeasures by a regional organization, verging on treating collective countermeasures as customary law. But if they are characterized as merely retorsion—lawful but unfriendly acts—they would not support the use of collective countermeasures as customary law. The deliberate ambiguity in the EU's legal framing may itself be a strategic choice, allowing the development of practice without committing the EU to a legal position. The distinction between countermeasures and retorsion is critical: as Focarelli (2016) has argued, much of the conduct cited as evidence of collective countermeasures may be more accurately characterized as retorsion, particularly where such collective countermeasures, such as travel bans and asset freezes, do not suspend legal obligations owed to the targeted state.

Legal Challenges

4.1 The Attribution Imperative

Attribution, the identification of the state responsible for a cyber operation, must be made before any countermeasure, whether individual or collective, can be taken. Under the ASR, countermeasures may be directed only at the state responsible for an internationally wrongful act, which necessarily means identifying the state responsible for the conduct in question, identified the rules of attribution codified in Articles 4–11 (ILC, 2001; Crawford, 2013). In cyber space, attribution is complicated by the technical ease with which the origin of operations can be concealed, or misdirected, the use of proxy actors and botnets, and the availability of false flag techniques.

It is important to distinguish among the different dimensions of attribution in cyberspace. *Technical* attribution uses forensic analysis to identify the origin of a cyber operation and its conduct. *Legal* attribution determines whether the conduct can be attributed to a state under the rules of the ASR (Articles 4–11). Finally, political attribution is the decision to publicly name the responsible actor, which involves both legal and strategic considerations. In short, then, a state may be identified as having *technically* conducted a cyber operation, but the operation may not be *legally* attributed to that state and, even if technically and legally attributable, the operation may not be *politically* (publicly) attributed to that state for a variety of legal and strategic reasons.

There is no agreement on the standard of proof required for *legal* attribution. In the 1949 *Corfu*

Channel case, the ICJ applied a demanding evidentiary standard to establish state responsibility before an international tribunal: although it found that the minefield "could not have been accomplished without the knowledge of Albania," it declined to attribute the physical mining of the channel to Albania itself, noting that such a grave charge against a state would require a degree of certainty that had not been reached. This distinction between knowledge and direct responsibility illustrates the complexity of the evidentiary inquiry, and it is debatable whether such a stringent standard is appropriate—or even practicable—for unilateral attribution decisions preceding countermeasures, particularly given the fast-moving nature of the cyber domain.

Many scholars and states have argued that a lower standard should apply in the cyber context, given the inherent difficulties of attribution. The Tallinn Manual 2.0 addresses attribution in multiple ways: Rule 15 governs the attribution of cyber operations by State organs, while Rules 6 and 7 require due diligence by states to ensure their territory is not used for cyber operations that adversely affects other states (Schmitt, 2017, Rules 6, 7, and 15). Some states may attribute responsibility on a case-by-case basis, considering the totality of the available evidence, and requiring that the victim state be "confident" in its attribution before responding. (United Kingdom, 2018). This approach implicitly accepts a lower threshold than the more familiar standards ("beyond a reasonable doubt" or "by a preponderance of the evidence") applied in formal adjudication before other tribunals.

Collective attribution mitigates some of these evidentiary challenges. When multiple states draw on their independent intelligence capabilities and technical expertise and agree, their collective judgment should carry greater evidentiary weight than any individual assessment. The coordinated attributions of WannaCry and NotPetya demonstrated this dynamic: for the first time, a group of states collectively assigned responsibility for destructive cyberattacks to specific nations—North Korea in the case of WannaCry and Russia in the case of NotPetya—and collectively carried out agreed-upon punitive measures, signaling the beginning of a coordinated effort to address the threat posed by global cyber operations (Efrony & Shany, 2018). However, collective attribution also raises concerns about "bandwagoning" the risk that states may join a collective attribution simply for political reasons, relying on the investigations and evaluations of other nations without independently verifying the evidence.

4.2 Proportionality in the Cyber Context

The principle of proportionality, codified in Article 51 of the ASR, requires that countermeasures be "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question." Applying this principle to cyber operations presents unique and rigorous challenges. The injuries caused by cyber operations are often difficult to quantify, particularly where the harm consists of the destruction of digital data, service disruptions, or the erosion of public confidence, rather than damage to physical infrastructure. The ICJ's approach in the Gabčíkovo-Nagymaros case provides a useful—if incomplete—framework for the cyber domain: the Court found that Czechoslovakia had "failed to respect the proportionality which is required by international law" by unilaterally assuming control of a shared resource and thereby depriving Hungary of its right to an equitable and reasonable share of the natural resources of the Danube, with continuing effects on the ecology of the riparian area (ICJ, 1997, para. 85). This case illustrates that proportionality is correctly assessed by reference to the concrete rights at stake and the actual effects of countermeasures on those rights.

The collective dimension of countermeasures makes calculation of proportionality even more complex. If, in response to a single wrongful act, multiple states respond to a single wrongful act with countermeasures against the same responsible state without coordinating their efforts, the cumulative effect may be disproportionate, even though each measure, taken individually, is proportional to the harm. However, existing law offers no clear solution to this 'aggregation problem' (Al-Kuwari, 2025), and the savings clause of Article 54 is silent on the conditions, such as proportionality, that should govern collective measures. As Focarelli (2016) has observed, understanding and applying of the proportionality requirement of Article 51 ASR to third-party countermeasures and, specifically, whether Article 51 requires some form of reasonable coordination among responding states to keep the collective response commensurate with the injury suffered have rarely been adequately examined. Logically, proportionality should be assessed at the collective level, weighing the totality of the

measures taken by all responding states against the gravity of the breach, rather than evaluating each state's response in isolation. However, assessment at the collective level requires that responding states coordinate their efforts and share information, which would surely be difficult to achieve in practice.

4.3 Protection of Third-Party Rights and Digital Infrastructure

The interconnected nature of digital infrastructure raises concerns about the impact of cyber countermeasures on states, private entities, and individuals that are neither the injured party nor the responsible state. Article 49(1) of the ASR requires that countermeasures be directed only at the responsible *state*, and the principle of necessity implies that they should avoid unnecessary harm to third parties, especially to those who are not "states." It is therefore crucial to distinguish between the rights and interests of third-party *states* (who have legal standing under international law) and those of private *actors* (whose protection is governed by domestic law and, in some cases, by international human rights law as well).

The impact of collective cyber countermeasures is particularly concerning, because coordination is complex and, especially, the risk of unintended consequences is high. The Tallinn Manual 2.0 addresses this issue in Rule 25, which strictly prohibits "a countermeasure that violates a legal obligation owed to a third State" (Schmitt, 2017, Rule 25). The proportionality requirement for countermeasures is separately addressed in Rule 23. At the same time, the commentary to Rule 25 acknowledges that the interconnected nature of the internet makes ensuring that cyber countermeasures do not have unintended spillover effects on third-party systems, and confining cyber operations to their intended targets, is particularly difficult.

Bridging the Gap: Toward a Legal Framework for Collective Cyber Countermeasures

5.1 The Theory of Third-Party Coercion

This article proposes that "third-party coercion" is a theoretically coherent framework for both understanding and, importantly, for justifying collective countermeasures in cyberspace. Traditional countermeasures theory conceives of the countermeasure relationship as strictly bilateral: the injured state exerts pressure on the responsible state to induce compliance. Third-party coercion extends this logic to situations in which other states that have not suffered injury, acting under Article 48 of the ASR, also take measures to force the responsible state to comply with its obligations toward the injured state or to the international community as a whole.

This framework draws on the work of Dawidowicz (2016), who identified a substantial body of state practice in which non-injured states have taken measures against responsible states in response to serious breaches of *erga omnes* obligations: economic sanctions (such as the freezing of assets belonging to Libya, Syria, and Russia), suspension of treaty rights (such as suspending Libya and Syria from the Arab League), and diplomatic measures. It also draws on the theoretical contributions of both Tams (2005), who demonstrated that all states appearing in proceedings before the International Court of Justice are entitled to invoke obligations *erga omnes* and to take countermeasures in response to serious *erga omnes* breaches, and of Sicilianos (2010), who examined the responses of non-injured states to grave breaches of *erga omnes* obligations, and the complex interplay between those responses and the role of the United Nations Security Council.

In the cyber context, third-party coercion is a particularly compelling approach. Many cyber-operations affect the international community as a whole, such as the targeting of critical internet infrastructure, global financial systems, and public health institutions. Rule 30 of the Tallinn Manual 2.0 acknowledges that any state may coerce compliance by a state whose cyber operations have breached an *erga omnes* obligation owed to the international community as a whole (Schmitt, 2017, Rule 30). This article further proposes, as a matter of progressive development, that what was once the prohibition of certain categories of cyber operations may evolve into recognition that they are *erga omnes* obligations, particularly where they target essential services or violate sovereignty. If this evolution continues, it will strengthen the foundation for collective countermeasures, allowing states entitled

under Article 48 to invoke responsibility to characterize third-party coercion as a "lawful measure" within the meaning of Article 54.

5.2 Conditions and Safeguards

Any framework for collective countermeasures in cyberspace must include robust conditions and safeguards to prevent abuse and to protect all parties and their legitimate interests. The existing conditions for individual countermeasures in the ASR include Article 52(1)(b), which requires prior notification before the use of countermeasures; Article 50, which prohibits the use of countermeasures; Article 49(3), which requires that countermeasures be reversible; and Article 52(3), which requires the parties to offer or submit to dispute resolution. This article draws on these existing conditions and adapts them to the context of collective cyber measures to propose the following:

First, collective countermeasures should be used only to respond to serious breaches of *erga omnes* or *erga omnes partes* obligations, consistent with the threshold established in Articles 40–41 of the ASR. Minor cyber incidents or ordinary violations of bilateral obligations should not enable a collective response. This threshold requirement safeguards against the proliferation and escalation of collective measures and ensures that they remain an exceptional response to exceptional circumstances.

Second, whenever collective countermeasures are being considered, the attribution of the wrongful act to the responsible state requires a heightened evidentiary standard. Given the risks of erroneous or politically motivated attributions, collective responses should require independent attributions by multiple sources, including technical evidence, intelligence analysis and, where available, assessment by an international or regional organisation.

Third, proportionality must be assessed at the aggregate level and must consider the cumulative effect of all measures taken by all responding states. This requires that responding states coordinate their responses, to ensure that their collective response remains commensurate with the breach.

Fourth, countermeasures, whether individual and collective, must protect both third-party rights and critical civilian infrastructure. Responding states should assess impacts before taking cyber countermeasures and should de-escalate when unintended harm to digital systems and networks is imminent. This extends the logic of Article 50 ASR, which prohibits countermeasures that affect fundamental human rights obligations, to encompass the protection of essential civilian digital services and digital infrastructure.

Fifth, collective countermeasures must be only temporary and directed only at inducing compliance, rather than inflicting punishment. The goal of countermeasures must be limited to inducing the responsible state to fulfil its international obligations, rather than punishing the responsible state (ILC, 2001, Commentary to Art. 49, para. 1). This limitation applies with equal force to collective measures and constrains the transformation of collective countermeasures into collective punishment.

Finally, in addition to these substantive conditions, collective countermeasures should be subject to procedural safeguards like those in ASR Article 52. Before taking collective countermeasures, responding states should (1) urge the responsible state to comply; (2) notify it that countermeasures are impending; and (3) offer to negotiate. Certainly the urgency of cyber operations may require adapting these procedural steps, particularly those requiring the urgent countermeasures necessary to preserve the responding states' rights. As contemplated by Article 52(2), the principle of prior engagement should not be abandoned entirely.

5.3 The Role of Regional Organisations

Regional organisations are well-positioned as institutional frameworks for the use of collective cyber countermeasures on a regional scale. The European Union's Cyber Diplomacy Toolbox already provides a model, albeit an imperfect one, for how a regional organisation can facilitate collective responses to cyber threats by constructing a framework of proportionate restrictive measures, calibrated to the scope, scale, duration, intensity, complexity, sophistication, and impact of the malicious activity (Council of the EU, Decision (CFSP) 2019/797, Recital 4). NATO's coordinated political response to the 2022 cyber-attacks on Albania, including NATO’s solidarity with and bilateral

support for its affected ally, illustrates how an existing security alliance can coordinate collective political support in response to cyber-attacks, even without a formal collective cyber-defense mechanism (NATO, 2022).

For regional actors, such as the Gulf Cooperation Council (GCC), which face significant and growing cyber threats from both state and non-state actors, the need for regional frameworks for collective cyber responses is both urgent and practical. The GCC Vision for Regional Security explicitly prioritizes objectives, such as raising cybersecurity levels, countering cybercrime, and establishing strategic partnerships with regional and international actors to bolster cybersecurity (GCC, 2024). ASEAN's experience with regional cybersecurity cooperation offers useful lessons, although these lessons come with caveats. ASEAN's approach, which emphasizes capacity building, information sharing, and implementing voluntary norms of responsible State behavior in cyberspace (ASEAN, 2021), operates within a cooperative framework very different from the collective countermeasures paradigm discussed in this article. Nonetheless, the institutional infrastructure developed using ASEAN-type cooperative models may, over time, support the development of more robust collective response capabilities.

The role of regional organizations can go far beyond coordinating collective cyber countermeasures. Regional frameworks can legitimize collective responses, adding a multilateral imprimatur to collective responses that might otherwise be perceived as unilateral coercion. Regional organizations can also assemble the information necessary to centrally assess proportionality and ensure that the collective response remains within lawful bounds. The development of regional norms and mechanisms for collective cyber responses may thus, over time, contribute to the formation of an international legal consensus on this subject.

Conclusions and Recommendations

This article examined the evolving intersection of collective countermeasures and state practice in cyberspace, revealing a significant and growing gap between the traditional bilateral framework of the ASR and the emerging reality of collective cyber responses. The analysis leads to several key conclusions and recommendations.

First, the current international legal framework, as reflected in the ASR and state position papers, does not explicitly authorize collective countermeasures, whether in cyberspace or otherwise. The savings clause of Article 54 was deliberately formulated "so as not to prejudice any position concerning measures taken in the general or collective interest," reflecting that there was no consensus when the ASR was adopted (ILC, 2001, Commentary to Art. 54, para. 7). This lack of consensus should not be read as a prohibition, nor can it be read as authorization. The evolving state practices: collective attributions, coordinated diplomatic responses, and institutional mechanisms such as the EU Cyber Diplomacy Toolbox, provide evidence that states are, in practice, already responding collectively to cyber operations (Dawidowicz, 2016; Council of the EU, Decision (CFSP) 2019/797). However, a fundamental question remains: are these responses countermeasures in the legal sense or retorsion, meaning acts that, although unfriendly, are not contrary to international law and therefore need not be justified as countermeasures (ILC, 2001; Crawford, 2013).

Second, the gap between law and practice is narrowing, albeit neither consistently nor steadily. Although some states and regional organisations have taken collective cyber responses, many states still lack a clear legal position on whether collective countermeasures are even permissible under international law, much less under what conditions. This complicates the assessment of *opinio juris*. As Dawidowicz (2016) has observed, the practice of third-party countermeasures was considered by the ILC to be too "deeply enmeshed with policy" and "too close to politics than to law to demonstrate that any such right existed," making it difficult to discern a clear *opinio juris*.

Focarelli (2016) goes further, questioning whether the law in this area is sufficiently formed to reach a consensus. These assessments caution against premature claims that an opinion concerning collective cyber countermeasures has even formed, much less constitutes a customary rule. Nevertheless, the trend toward greater collective action is unmistakable, and the question is

increasingly not whether, but when and under what conditions, and with what safeguards, collective countermeasures have become an accepted feature of the international legal framework governing cyber operations.

Third, the theory of third-party coercion offers a framework for conceptualizing collective countermeasures in cyberspace that is both practically viable and legally grounded. By grounding collective action in the rights of non-injured states, under both Article 48 of the ASR and the savings clause of Article 54, this framework works within the existing legal architecture, while also acknowledging what the ILC Commentary itself notes: that "State practice is sparse and involves a limited number of States" and that the current state of international law on countermeasures in the collective interest "is uncertain" (ILC, 2001, Commentary to Art. 54, para. 6). The conditions and safeguards proposed in this article, including the requirement of a serious breach of *erga omnes* obligations (consistent with Articles 40–41 ASR), heightened attribution standards, assessment of proportionality on an aggregate basis, third-party protections, procedural requirements analogous to Article 52 ASR, and limitations on the purpose of the use of collective countermeasures (inducing compliance rather than punishment, consistent with Article 49(1) ASR), provide a structured approach to collective countermeasures that balances effectiveness with restraint.

Fourth, regional organisations can play a critical role in both institutionalizing and legitimizing collective cyber responses. The EU Cyber Diplomacy Toolbox and NATO's coordinated political responses provide models to be adapted and developed by other regional organisations. The GCC and ASEAN, in particular, face growing cyber threats that demand collective responses, and the development of regional frameworks for collective cyber countermeasures should be a priority for these organisations and others like them.

Based on these conclusions, this article recommends: (a) that states continue to develop and publicly articulate their legal positions on collective countermeasures in cyberspace, as transparency in state practice and *opinio juris* is essential for the progressive development of international law; (b) that regional organisations invest in the development of institutional frameworks for collective cyber responses, drawing on existing models while adapting them to their own regional circumstances; (c) that the international community work toward establishing clearer standards for collective attribution, including mechanisms for independent verification and quality assurance; and (d) that scholarly and policy attention be directed toward the practical implementation of proportionality and third-party protection standards in the context of collective cyber countermeasures, as these remain among the most technically and legally complex aspects of the emerging framework.

This article is subject to certain limitations to be acknowledged. The analysis draws primarily on the state practice and legal positions of Western states and their allies, with only limited attention given to the perspectives of China, Russia, and states in the Global South, whose positions on collective countermeasures may differ significantly from those of Western states and their allies. The theoretical framework of third-party coercion, although ostensibly grounded in existing legal scholarship, remains untested in practice. Moreover, the rapid evolution of cyber practice and state positions necessarily makes the empirical basis for the analysis only a snapshot of a dynamic and evolving field. Future research should expand the geographical scope of inquiry, test the proposed framework against emerging state practice, and develop more detailed proposals for the institutional mechanisms through which collective cyber countermeasures might be coordinated and regulated.

The evolution of digital international relations demands that the legal frameworks that govern state behavior also evolve. Collective countermeasures in cyberspace are a significant step in this evolution. By closing the gap between state practice and international legal frameworks, the international community can respond more effectively to the cyber threats of the twenty-first century..

References

Alland, D. (2002). Countermeasures of General Interest. European Journal of International Law, 13(5), 1221–1239. https://doi.org/10.1093/ejil/13.5.1221

Al-Kuwari, K. (2025). Collective countermeasures and regional cooperation: Strengthening cybersecurity in Qatar

and the Gulf Cooperation Council, Doctoral dissertation, University of Bradford. https://bradscholars.brad.ac.uk/handle/10454/20714

ASEAN Secretariat. (2021). ASEAN Cybersecurity Cooperation Strategy 2021–2025. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Council of the European Union. (2017). Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox). ST-10474-2017-INIT. https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf

Council of the European Union. (2019). Council Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0797

Crawford, J. (2013). State Responsibility: The General Part. Cambridge University Press. https://doi.org/10.1017/CBO9781139033060

Cybersecurity and Infrastructure Security Agency (CISA). (2022). Iranian Cyber Actors Conduct Cyber Operations Against the Government of Albania (Advisory AA22-264A). https://www.cisa.gov/sites/default/files/publications/aa22-264a-iranian-cyber-actors-conduct-cyber-operations-against-the-government-of-albania.pdf

Dawidowicz, M. (2016). Third-Party Countermeasures: A Progressive Development of International Law? QIL, Zoom-in, 29, 3–15. https://www.qil-qdi.org/wp-content/uploads/2016/06/02_Collective-CM_DAWIDOWICZ.pdf

Deeks, A. (2020). Defend Forward and Cyber Countermeasures. Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper, No. 2004. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3670896

Efrony, D., & Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. American Journal of International Law, 112(4), 583–657. https://doi.org/10.1017/ajil.2018.86

Estonia, Ministry of Foreign Affairs. (2019). Estonia's Position on the Application of International Law in Cyberspace. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Estonia_(2019)

Focarelli, C. (2016). International Law and Third-Party Countermeasures in the Age of Global Instant Communication. QIL, Zoom-in, 29, 17–23. https://www.qil-qdi.org/wp-content/uploads/2016/07/03_Collective-CM_FOCARELLI_FIN.pdf

France, Ministère des Armées. (2019). Droit international appliqué aux opérations dans le cyberspace. https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)

Gulf Cooperation Council Secretariat General. (2024). GCC Vision for Regional Security (2nd ed.). https://gcc-sg.org/ar/MediaCenter/DigitalLibrary/Documents/27848330-555a-4a7d-9a6c-206b797fd2f9.pdf

ICJ. (1949). Corfu Channel Case (United Kingdom v. Albania). ICJ Reports 4. https://www.icj-cij.org/node/103099

ICJ. (1997). Gabčíkovo-Nagymaros Project (Hungary/Slovakia). ICJ Reports 7. https://www.icj-cij.org/node/103193

ILC. (2001). Articles on the Responsibility of States for Internationally Wrongful Acts, with Commentaries. UN Doc. A/56/10. https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf

ILC. (2018). Conclusions on Identification of Customary International Law, with Commentaries. UN Doc. A/73/10. https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf

Ireland, Department of Foreign Affairs. (2023). Ireland's Position on the Application of International Law in Cyberspace. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Ireland_(2023)

NATO. (2022). North Atlantic Council Statement on the Situation in Albania. Press Release (2022) 134, 8 September 2022. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/09/08/statement-by-the-north-atlantic-council-concerning-the-malicious-cyber-activities-against-albania

Netherlands, Ministry of Foreign Affairs. (2019). Letter to the Parliament on the International Legal Order in Cyberspace (July 2019). https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_Netherlands_(2019)

Poli, S., & Sommario, E. (2023). The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions. German Law Journal, 24(3), 522–536. doi:10.1017/glj.2023.25

Rama, E. (2022). Statement by the Prime Minister of Albania on the Severance of Diplomatic Relations with Iran. Official Statement, September 2022. https://allarab.news/albania-formally-cuts-ties-with-iran-and-how-this-impacts-the-region/

Schmitt, M.N. (Ed.) (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

https://doi.org/10.1017/9781316822524

Schmitt, M.N. (2019). The Netherlands Releases a Tour de Force on International Law in Cyberspace. Just Security, 9 September 2019. https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/

Schmitt, M.N., & Watts, S. (2021). Collective Cyber Countermeasures? Harvard National Security Journal, 12(2), 373–411. https://harvardnsj.org/wp-content/uploads/2021/07/HNSJ-Vol-12-Schmitt-and-Watts-Collective-Cyber-Countermeasures.pdf

Sicilianos, L.-A. (2010). Countermeasures in Response to Grave Violations of Obligations Owed to the International Community. In J. Crawford, A. Pellet, & S. Olleson (Eds.), The Law of International Responsibility (pp. 1137–1148). Oxford University Press. https://doi.org/10.1093/law/9780199296972.003.0098

Tams, C.J. (2005). Enforcing Obligations Erga Omnes in International Law. Cambridge University Press. https://doi.org/10.1017/CBO9780511494116

United Kingdom, Attorney General's Office. (2018). Cyber and International Law in the 21st Century. Speech by the Attorney General. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

.