Responding to Proxy Cyber Operations Under International Law

Lieutenant Colonel Durward E. Johnson
Professor Michael N. Schmitt

INTRODUCTION

The United States (US), its allies, and other partners are engaged in long-term strategic competition with Russia and China—near-peer adversaries adept at operating in the grey zone of international law, where the precise contours of the law are difficult to discern.[1] They do so to complicate our response options, in part to avoid provoking a direct military response.[2] Increasingly, cyberspace is that grey zone, a domain in which Russia, China, and other adversaries such as Iran and North Korea mount cyber operations ranging from cyber-enabled espionage, theft, and propaganda campaigns to significantly more disruptive and destructive operations. In particular, they often leverage non-state actors—cyber proxies—to do their bidding because proxies further complicate legal and policy assessments of the operations. And those assessments determine the response options available to victim states.

As a general matter, states agree that they "must not use proxies to commit internationally wrongful acts...[and] should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs [information and communications technology]."[3] The legal challenge is that the nature of proxy use differs from case to case, and these distinctions determine the lawfulness of responses. Russia's relationship with proxy groups provides a good example. At one end of the spectrum lies tacit approval of hostile cyber operations conducted independently by non-state patriotic hackers. Recall the large-scale denial of service (DDoS) cyber operations against Estonia in 2007 that shut down, among other things, government websites, key banks, and news outlets. Although the extent of its involvement remains murky, Russia's failure to condemn the operations and take measures to terminate those mounted from its territory evidence at least tacit approval.[4]

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

But the paucity of evidence as to Russian government involvement or control not only allowed Russia plausible deniability but also severely limited its adversaries' response options. At the other end of the spectrum, Russian security and intelligence services have directed hostile cyber operations by cyber proxies.[5] An example is the massive Yahoo data breach that began in 2014. Three years later, a U.S. federal grand jury indicted two Russian Federal Security Service officers for conspiring with cybercriminals to commit cybercrime and espionage.[6]

The relationships between proxy groups and governments usually fall between these extremes. Sometimes, states employ a multifaceted approach, as Russia did in its 2020 U.S. federal elections influence campaign, which included operations by "Russia's intelligence services, Ukraine-linked individuals with ties to Russian intelligence and their networks, and Russian state media, trolls, and online proxies."[7] Other recent incidents in which the precise extent and nature of Russian government involvement remains an open question include the Colonial Pipeline and JBS ransomware operations.

This article addresses an issue appearing in the Army's 2021–22 Key Strategic Issues List: "*Assess Russia's use of proxy or patriotic hackers and evaluate international laws and norms that can be used to limit their use*."[8] As will be illustrated, it is generally the interplay between the type of harm caused by a hostile cyber operation, the legal attributability of the operation to a state, and the legal nature of the proposed response that determines how the victim state may respond. Analysis begins with a discussion of the international rules most likely to be violated by either a proxy's hostile cyber operation or the proposed cyber response by the victim state. Those response options will also be determined by whether the proxy's operation can be attributed to a state as a matter of law, the subsequent topic addressed

Michael N. Schmitt is Professor of International Law at the University of Reading in the United Kingdom, G. Norman Lieber Distinguished Scholar at the U.S. Military Academy at West Point, Charles H. Stockton Distinguished Scholar-in-Residence at the U.S. Naval War College, NATO Cooperative Cyber Defense Center of Excellence Senior Fellow, and Strauss Center Distinguished Scholar and Visiting Professor of Law at the University of Texas. The Director of the Tallinn Manual 3.0 Project, Schmitt serves on the Department of State's Advisory Committee on International Law, is a member of the Council on Foreign Relations and a Fellow of the Royal Society of Arts. Follow him on Twitter (@Schmitt_ILaw).

below. Such legal attribution must not be confused with technical attribution, which denotes evidence of the relationship, and from political attribution, which simply refers to a policy decision to blame another state. The foundation laid, the discussion will proceed serially through the various categories of responses existing in international law, zeroing in on the legal preconditions that must exist before engaging in them against a proxy group or the affiliated state.

Two points must be made at the outset. First, "proxy" is not a legal term. Instead, international law asks more specifically about the relationship between the non-state actor and the state concerned. As used in this article, "proxy" simply refers to an individual or group with some link to a state. Whether a proxy's hostile cyber operations are legally attributable to a state depends on the attendant circumstances, which will be outlined below.

Second, the analysis is not limited to Russian use of proxies, for the identity of the state that has resorted to their use is irrelevant in international law pursuant to the principle of sovereign equality. The analysis that follows is as applicable to the use of proxies by states such as China, Iran, and North Korea as it is to Russia.[9]

Unlawful Cyber Operations

The range of lawful response options in the face of proxy cyber operations is determined in part by 1) whether the proxy's operation constitutes an "internationally wrongful act" (unlawful cyber operation) by the affiliated state, 2) whether the victim state's proposed cyber response is unlawful, and 3) the existence of any "circumstances precluding wrongfulness," a legal term of art, that would render lawful the victim state's otherwise unlawful response to the cyber operation directed against it.

There are scores of international law rules that hostile cyber operations, or responses to them, might violate.

The *Tallinn Manual 2.0* project sponsored by the NATO Cooperative Cyber Defence Centre of Excellence identified many.[10] They range from violations of diplomatic or international human rights law to cyber operations that breach the obligations found in the law of the sea, air, or outer space. Excluding violations of the law of armed conflict, three loom large—the obligation to respect the sovereignty of other states, the prohibition on coercive intervention, and the use of force.[11]

Most international law rules, including the three key ones, apply only to states. Although the cyber operations of non-state groups can be criminal acts under the laws of a state that enjoys jurisdiction, without attribution of the cyber operation to a state as a matter of law, there is generally no international law violation. In other words, the question in the proxy context is whether the proxy's operation would breach one of these rules had the state itself conducted it and, if so, whether the proxy's conduct is legally attributable to the state. Before turning to attribution, therefore, the first step is to examine when cyber operations breach international law obligations.

The most likely obligation to be breached by a cyber operation is respect for another state's sovereignty. There has been some controversy regarding whether violation of sovereignty is even a rule of international law, with the United Kingdom suggesting in 2018 that it is not.[12] The United Kingdom argues that a state's remotely-conducted cyber operation into another state's territory does not violate its sovereignty, irrespective of the consequences of the operation; accordingly, neither would a proxy's operation. Since then, every state that has taken a firm stance on the matter accepts the existence of a rule of sovereignty. NATO's Cyber Doctrine even reflects the rule.[13] The US position, however, remains ambiguous.[14] Yet when the United Kingdom issued a "reservation" (a statement of disagreement) regarding NATO's acknowledgment of the rule, the US did not.[15]

From a legal perspective, the better view is that a rule of sovereignty exists. As a general matter, there are two ways a cyber operation can violate sovereignty. First, a cyber operation can do so based on territoriality. This occurs when a state's cyber operation, or a proxy's operation attributable to a state, causes certain effects on another state's territory. Physical damage or injury, as well as permanent loss of functionality, clearly suffice. Whether remotely causing effects that do not reach this level violates sovereignty remains an open question that will only be settled once states publicly begin to set forth their views on the matter.[16] For instance, there is no consensus about whether temporarily interfering with the cyberinfrastructure's functionality or causing it to operate in other than the intended manner qualifies. That said, there is agreement that the rule protects both private and public infrastructure. Additionally, the requisite effects can be caused indirectly. As an example, a cyber operation against a state's COVID-19 management system will violate sovereignty if it results in illness or death that might otherwise have been avoided.[17]

Second, interference with, or usurpation of, an inherently governmental function violates

sovereignty.[18] Inherently governmental functions are those that only a state has the authority to perform. Examples include conducting elections, tax collection, law enforcement, national crisis management, diplomacy, and national defense. Interference occurs when the cyber operation makes it materially more difficult to perform the function, as in temporarily disrupting the operation of election machinery or interfering with defensive military systems like early-warning radars. Usurpation involves performing inherently governmental functions in lieu of the other state, as in conducting law enforcement measures against proxies, such as remote searches or virtual seizure in another state's territory without that state's permission.

Unlike sovereignty, the rule of non-intervention is uncontroversial, with all states accepting its application in the cyber context. Intervention has two elements. First, the cyber operation has to involve a state's internal or external affairs (the so-called *domaine réservé*[19]). These are areas of activity that international law leaves to states to regulate, such as the state's political, economic, and social policies. Second, the hostile cyber operation in question must be coercive in the sense of depriving the victim state of choice by forcing it to (a) adopt a policy it would not otherwise adopt (b) refrain from adopting one it would otherwise adopt or (c) execute a policy in a manner that differs from that intended. Mere persuasion, influence, or diplomatic pressure is insufficient, as are propaganda and most other information operations, even when untruthful. Cyber operations motivated by other than a desire to address policy choice or execution, such as those that are purely criminal, as is often the case with North Korean operations,[20] also do not qualify.

Absent either element, a proxy's cyber operation, whether attributable to a state or not, does not violate the intervention rule (although it might violate other rules, such as sovereignty). For example, it is not intervention to use proxies to engage in an information campaign that benefits a candidate during another state's election, but it would be to have them manipulate election machinery or provide false but believable information as to how to vote online (when online voting is not allowed).[21]

In extreme cases, a proxy's cyber operation that is legally attributable to a state could violate the customary law prohibition on the use of force codified in Article 2(4) of the UN Charter. All states agree that the prohibition applies in the cyber context; the challenge lies in identifying those operations crossing the use of force threshold. And as with the sovereignty and intervention rules, a proxy's cyber operation must be attributable to a state to violate the use of force prohibition. If it is not, it is mere criminality under the domestic laws of states having jurisdiction over the matter.

There is broad agreement that a cyber operation causing physical damage or injury beyond a *de minimis* level amounts to a use of force, as would an operation causing substantial loss of a targeted system's functionality. Below that threshold, consensus among states has proven elusive. Increasingly, they are adopting a case-by-case approach that assesses the "scale and effects" of a cyber operation to determine whether it crosses the use of force line.[22]

The adoption of this approach is significant, for it signals that in the view of these states, there may be proxy cyber operations that are neither destructive nor injurious but that nevertheless qualify as uses of force. France, for example, has taken the position that a cyber campaign resulting in severe nationwide economic disruption could qualify as such, and the Netherlands has hinted that it is willing to come to the same conclusion.[23] By this approach, states will look at an array of non-exclusive factors in deciding whether a proxy's cyber operation is of sufficient scale and if the effects amount to a use of force by the state to which it is attributable. The factors that will be considered include, but are not limited to, the severity of consequences, the geopolitical situation, the track record of the state engaging in the cyber operation, the immediacy and directness of its effects, the entity launching the operation (e.g., military, intelligence, proxy), and the target. However, until states begin to add granularity to their position, the legal character of a particularly severe but non-destructive or injurious cyber operation will remain uncertain.

Importantly, espionage, as such, does not violate international law. Therefore, neither a proxy's cyber espionage nor espionage by a victim state used to fashion a response is unlawful. That said, if the consequences of the espionage qualify as a violation of international law, for instance, because it damages the targeted cyberinfrastructure or is being used for law enforcement purposes (both sovereignty violations), the operation will be unlawful on that basis. Thus, whether a cyber operation has breached an international law obligation is sometimes uncertain. Nevertheless, determining whether a proxy's hostile operation or a state's response to such an operation breaches international law is a necessary first step in identifying lawful response options.

Attribution

The second step in identifying response options is determining whether a proxy's cyber operation is attributable to a state under international law. As explained, establishing international law violations requires both a breach of an international law obligation and attribution of the cyber operation in question to a state (labeled the "responsible state" in international law terms). Only after deciding whether the proxy's operation satisfies both criteria, and whether a particular response by the victim state (the "injured state") would breach any legal obligation itself can the full range of response options for a specific incident be identified.

There are multiple bases for attributing a proxy's cyber operations to a state. To begin with, individuals, groups, or other entities are considered *de facto* organs for purposes of legal attribution if they are completely dependent on the state, as when an intelligence agency creates an unofficial group for the express purpose of conducting hostile cyber operations, funds (perhaps secretly) the group, and determines its operations.[24] In these cases, a proxy is essentially an instrument of the state.[25] Cyber operations are also attributable to a state where individuals, groups, or entities are legally empowered by the state to "exercise elements of governmental authority."[26] The activities must be quintessentially governmental. An example would be

contracting with a private company to perform non-commercial cyber espionage on behalf of the state or conduct offensive cyber operations against the state's adversary.

In both of these situations, even proxy cyber operations that are *ultra vires,* that is, beyond the scope of the authority granted by the state, are attributable to it so long as they are related to the activity. For example, if a company is hired to conduct offensive operations (a quintessential governmental activity) but instructed not to target particular government cyberinfrastructure, yet it nevertheless directs operations against that infrastructure, the state will be responsible for the operations. But if the company engages in classic cybercrime for its own profit, the state will not bear responsibility.

The most common basis for legally attributing proxy cyber operations to a state is when they are conducted "on the instructions of, or under the direction or control of, that state."[27] Acting on a state's instructions generally occurs when a state recruits or instigates a proxy to perform as its "auxiliary" without having any official or legal connection to that state.[28] For instance, the state could recruit a group of volunteer patriotic hackers to supplement its cyber actions, as in conducting espionage that supports the state's hostile operations. As a matter of law, the state would be responsible for the hostile cyber operations conducted by the proxy.

The "direction or control" standard applies when the proxy's affiliation with the state is looser than that of a proxy acting as an auxiliary. In its *Nicaragua* judgment, the International Court of Justice suggested that a proxy's acts are attributable when the state directs or controls specific operations; the Court labeled this "effective control." General support or encouragement of cyber proxy operations is not enough.[29] The Court even held that a state's participation in the "financing, organizing, training, supplying, and equipping" of a proxy organization and "the selection of its military or paramilitary targets, and the planning of the whole of its operation" did not reach the "effective control" threshold.[30] Such involvement in the cyber operations would likely amount to unlawful intervention into the internal affairs of the target state, but the proxy's actions themselves would not be attributable to the state concerned.

Finally, a proxy's cyber operation is attributable as a matter of law to a state when the latter "acknowledges and adopts the conduct in question as its own."[31] The standard requires the state to acknowledge, through words or conduct, that the hostile cyber operation occurred. It must also adopt the proxy's operation by taking affirmative steps to protect or otherwise facilitate its continuation. This happens in very limited situations, for states typically use proxies so they can distance themselves from the hostile cyber operation.

Assessing whether the nature of the relationship between a cyber proxy and a state satisfies the requirements for legal attribution is challenging due to the high thresholds of the various attribution rules and the difficulty of factually establishing the nature of the relationship between the proxy and the state. Complicating matters is the absence of any agreed-upon evidentiary threshold for attribution (unless the case is before a court), disagreement as to whether reasonable but mistaken attribution renders a countermeasure (see below) unlawful, and the

fact that international law does not require states to produce the evidence upon which they base attribution. Nonetheless, only after an attribution determination has been made is it possible to identify the available response options. It is to those options that the discussion turns.

Retorsion and Other Lawful Responses

The most common responses to hostile cyber operations are "acts of retorsion"—unilateral actions that do not violate international law per se, although they are "unfriendly" from the perspective of the entity against which they are directed.[32] Examples include economic sanctions, canceling state visits, expelling diplomats, or even severing diplomatic relations. By way of illustration, when Russia targeted the US with cyber election interference in 2016, including through the use of proxies like the Internet Research Agency, the Obama Administration responded by imposing sanctions, expelling "diplomatic" personnel, and closing Russian facilities in the US.[33] Similarly, the Biden administration has elected to reply to the 2020 Russian election-related cyber operations and the SolarWinds campaign utilizing retorsion.[34]

Retorsion options are an especially useful response to a hostile state or proxy cyber operation that either does not violate international law or is of an ambiguous legal character, as with operations like SolarWinds.[35] Moreover, a state need not legally attribute a proxy's operation to another state before engaging in acts of retorsion against the proxy, its members, or a state it suspects of involvement; it even would be lawful to sanction them based on mere suspicion of involvement, assuming doing so is compliant with the state's domestic law. Simply put, acts of retorsion are always available response options because they are lawful measures unconstrained by the international legal requirements that accompany more robust self-help measures discussed below. Of course, a responsible member of the international community should only engage in retorsion when reasonable in the circumstances and in good faith.

Economic sanctions are a prominent means of retorsion and a core element of US strategy to deter Russia's use of cyber proxies and other malicious behavior. The US generally relies on Executive Order (EO) 13694 as amended by EO 13757, which was codified in the Countering America's Adversaries Through Sanctions Act (CAATSA), to sanction Russians and Russian entities that have engaged in hostile cyber operations.[36] Section 224 of CAATSA expressly authorizes sanctions against cyber proxy operations conducted on behalf of the Russian government that undermine "cybersecurity against any person, including a democratic institution, or government."[37] Hundreds of proxy group members and Russian security and intelligence services personnel have been sanctioned for having conducted cyber operations using these authorities.[38]

Cyber responses that do not cause effects that would violate international law also qualify as acts of retorsion. For instance, a state targeted by a proxy's cyber operations may undertake cyber information (and even disinformation) campaigns,[39] cyber espionage, and other intelligence and counterintelligence cyber operations against both a proxy or a state with some

relationship to the hostile operations, so long as the cyber responses do not cross any legal threshold, such as those described above, that would render them unlawful.[40] Or a targeted state could establish access within hostile cyberinfrastructure without causing internationally wrongful effects to signal its capability and willingness to respond to future hostile cyber operations.[41] The victim state could even block access by proxy groups, individuals, and specified states to its cyberinfrastructure as an act of retorsion, for there is no international law right of access to cyberinfrastructure on another state's territory.[42]

Other lawful means of responding to proxy cyber operations are available. For instance, the United States is increasingly resorting to judicial action by indicting members of proxy groups for domestic criminal offenses, as in the case of the Yahoo data breach mentioned above[43] and a 2019 criminal indictment of two members of Evil Corp, a Russian-based cybercriminal organization accused of supporting the Russian government's hostile cyber efforts.[44] The targeted state can also seek a UN Charter, Chapter VII, Security Council resolution condemning proxy operations and authorizing interference, disruption, or even destruction of a proxy's cyber capabilities, as well as sanctions or other action against a state supporting the group.[45] Of course, doing so in the case of Russia or China would be impossible in light of their veto power as one of the permanent five (P5) members of the Security Council. Judicial action in the International Court of Justice against a state to which a proxy's operations are attributable is a theoretical possibility, although highly unlikely because of the jurisdictional hurdles of bringing another state before that court.[46]

States are inclined to resort to the retorsion option or judicial action to respond to hostile proxy cyber operations, not only because they are a lawful option when reacting to hostile cyber operations that do not violate international law, but they also minimize political and legal risk in situations where there is uncertainty as to whether the proxy's cyber operation is unlawful. Moreover, factual evidence of attribution may be difficult to acquire, or the legal threshold for attribution may not have been reached in a case where a foreign state's involvement is suspected. Conducting acts of retorsion against that state is nevertheless permissible, while most other self-help measures would not be. Such measures may prove inadequate, however, in limiting or deterring the use of cyber proxies, for they generally impose limited repercussions, thereby necessitating an understanding of other measures of self-help.

Countermeasures

In certain circumstances, a state might need to take more robust measures—such as countermeasures, actions undertaken out of necessity, or self-defense—in the face of proxy cyber operations. Each of these responses would otherwise violate international law, but international law treats them as "circumstances precluding wrongfulness."[47] In other words, responses against the responsible state in the underlying circumstances are justified or excused under international law even though they are technically unlawful acts, so long as strict legal criteria for each are met, as we will discuss below.

Countermeasures are otherwise unlawful actions that international law nevertheless allows an injured state to take to compel a responsible state to stop its unlawful conduct or to provide reparations (including compensation) for any harm caused.[48] For example, an injured state may respond to the proxy's unlawful cyber operation with its own cyber operation that violates the sovereignty of a state responsible for a proxy's operations. The operation could even take the form of a violation of the responsible state's sovereignty by conducting operations against the proxy's cyberinfrastructure on the responsible state's territory.

Countermeasures are by definition violations of international law, they are subject to stringent limitations. First, they are only available against hostile cyber operations that are internationally wrongful acts. In the proxy context, that means the proxy's hostile cyber operation must breach an international law rule and be legally attributable to a state before countermeasures are on the table. In the event of misattribution, the prevailing view is that the purported countermeasure is itself unlawful because there was no "circumstance" to "preclude its wrongfulness."[49]

Additionally, a desire to retaliate against the state to which the proxy's operations are attributable cannot be the predominant motivation for countermeasures; the primary purpose instead must be to directly terminate the hostile cyber operations or influence the responsible state to end the proxy's cyber operations (or provide reparations). This being so, cyber responses unlikely to end the proxy's hostile operations or cause the responsible state to offer reparations do not qualify as countermeasures; they are unlawful. Further, since countermeasures are meant to return a situation to one of compliance with international law, they are only available while the responsible state's unlawful cyber operation (including by a proxy), is underway. For the same reason, a state may not take them once that operation or a series of related unlawful operations (a cyber campaign) are complete.

Countermeasures also must be proportionate in the sense that they have to be "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[50] In other words, the pain inflicted on the responsible state by the state taking the countermeasure must be roughly equal in scope and severity to that suffered as a result of the former's operations or those of its proxy. Further, it is now well accepted that countermeasures may not involve the use of force; only non-forcible measures are permitted as countermeasures.[51]

Several issues surrounding countermeasures remain unsettled in law. For instance, there is no consensus about whether an injured state has a legal obligation to attempt lesser measures, such as cyber retorsion or countermeasures with less severe consequences, before employing countermeasures. Most of the *Tallinn Manual 2.0* experts believed that no such obligation exists, but it remains an open issue.[52] There is also a degree of uncertainty about when an injured state must notify the responsible state that it intends to take countermeasures. Generally, notification must precede the taking of countermeasures unless they are urgent.[53] In the

cyber context, states have been interpreting this exception very broadly because of the speed with which cyber operations unfold and the fact that notice may provide an adversary critical information regarding the injured state's cyber capabilities.[54] Yet, in fairness, advance notice makes some sense in the cyber proxy context, where there may be intentional efforts to spoof or mask origin and affiliation with a state. Notice would allow the state against which countermeasures are to be taken to offer evidence that it is not responsible for the proxy's operations, perhaps even by cooperating with the targeted state. The best view, and one balancing the interests of states, is that notice should not be required if infeasible in the circumstances.

The most significant unsettled issue is whether collective countermeasures are permissible, much like the UN Charter and customary law permit collective defense in response to an armed attack.[55] The question is whether a state targeted by a proxy's unlawful cyber operation that is attributable to another state may look to third states for help in conducting countermeasures, either by assisting or by engaging in countermeasures on behalf of the injured state. States are split (or non-committal) on the issue. For instance, Estonia takes the position, understandably in light of its vulnerability to hostile cyber operations by Russia and its proxies, that it may seek help from other states in taking countermeasures; NATO-ally France takes the opposite position.[56] As a matter of law, the better position is that collective countermeasures are permissible, but the paucity of state views on the matter means it remains an open question.[57]

Several illustrations are helpful to explain the taking of countermeasures. For cyber proxy operations originating from within another state's territory, countermeasures could consist of "hack backs" or other cyber responses targeting the source of the initial hostile operation. Suppose a hacker group located in and acting on state A's instructions is the source of a hostile cyber operation causing loss of functionality of private cyberinfrastructure in state B (a violation of its sovereignty). In that case, the latter may target the private hacker group's cyberinfrastructure in state A to shut it down. The operation would otherwise violate that state's sovereignty, but its wrongfulness is precluded by its status as a proportionate countermeasure.

However, countermeasures need not be directed at the source of the initial cyber operation. They may proportionately target any cyberinfrastructure located within the state to which the proxy's operations are attributable, whether government or privately-owned, to influence the responsible state to compel its proxy to desist (or to secure reparations from that state). The response need not even violate the same legal obligation. For instance, a proxy's attributable cyber operation against private cyberinfrastructure that violates another state's sovereignty could be responded to through cyber operations against the responsible state's satellites in a manner that contravenes space law. Similarly, non-cyber countermeasures (like the denial of landing rights provided for in a treaty or the closure of the territorial sea to "innocent passage" by the state's vessels) are permissible in the face of unlawful cyber operations (and vice-versa).[58]

Cyber proxies do not always operate from within the territory of the state to which their operations are attributable. When proxies operate from a third state, the injured state may employ

countermeasures directed at targets located in the responsible state's territory. A targeted state might, however, prefer to take action against the proxy's operations in the third state. The legal problem is that countermeasures may only be directed against a state that has breached a legal obligation owed to the state taking the countermeasures. Since countermeasures are otherwise unlawful actions, they would seem to be unlawful vis-à-vis the territorial state. The remedy to this situation can sometimes be found in the rule of due diligence.[59] States either disagree on the existence of such a rule or have not opined on its existence.[60] Nevertheless, the weight of opinion is that such a rule exists and is of particular relevance in the cyber context.

By it, states must put an end to ongoing cyber operations either mounted from or conducted remotely through cyberinfrastructure located on their territory whenever it is feasible for them to do so in circumstances where the operations are causing "serious adverse consequences" for a legal right of another state (such as sovereignty). This obligation does not require that the hostile cyber operation be legally attributable to a state, although it may be. And this is crucial because if a state uses a proxy from its own or another state's territory, but attribution cannot be established or the relationship does not reach the legal threshold for attribution, the due diligence rule may open the door to countermeasures.

To illustrate, assume cyber proxies are operating from one (territorial) state to intervene in the target state's elections unlawfully. The territorial state knows of the operations and can stop them. Yet, it fails to do so because it sympathizes with the proxy group, is allied with the responsible state, or for any other reason. The territorial state is in breach of its due diligence obligation. The injured state may take countermeasures against the territorial state to convince it to comply with its due diligence obligation to end the proxy's operations or even conduct operations against the proxy itself. In such a situation, the injured state's otherwise unlawful action (perhaps a breach of sovereignty) would be precluded because it qualifies as a countermeasure against the territorial state's non-compliance with the rule of due diligence.

A significant issue here is how to interpret the requirement that the taking of action be feasible before the due diligence obligation is breached. In this regard, the territorial state need only look to its own capabilities, such as technical solutions, classic law enforcement, instructing an Internet Service Provider to terminate service to the proxy, or even retaining the services of a private company that can terminate the proxy's operations. However, it need not accept assistance from the injured or other states; feasibility is assessed based on the state's capabilities alone.[61]

Actions Taken Out of Necessity

Targeted states may not have the option of employing countermeasures because the proxy's cyber operation does not violate international law, attribution cannot be established, or it is not feasible for the territorial state to terminate the proxy's operation and is therefore not in breach of any due diligence obligation. In these situations, the targeted state may take action based on a plea of necessity.

Plea of necessity actions are similar to countermeasures in that a state targeted by certain hostile cyber operations is permitted to respond in a manner that would otherwise violate international law; it is a "circumstance precluding the wrongfulness" of the response. States may do so in exceptional situations where cyber operations, including those mounted by proxies, create a "grave and imminent peril" to an "essential interest" of the targeted state, and the proposed response is the sole means of addressing the situation.[62]

Unlike countermeasures, the hostile cyber operation need not constitute an internationally wrongful act. This has two significant consequences. First, a hostile cyber operation does not have to breach any particular obligation of a state. Thus, uncertainty about whether a hostile cyber operation breaches an obligation such as respect for sovereignty or refraining from intervention, or certainty that it does not, is no obstacle to acting based on necessity.

Second, in the proxy context, unlike in regards to countermeasures, it is unnecessary to legally attribute the hostile cyber operation to a state before responding based on necessity. Indeed, there is no requirement to attribute the cyber operation to any particular entity at all. The sole requirement is a factual determination that the cyber operation, irrespective of who might have launched it, gravely threatens an essential interest of the targeted state, and the proposed response is the only feasible means to prevent or end the intrusion.

For instance, consider a proxy cyber operation targeting essential cyberinfrastructure, such as the national financial system, launched from a state to which attribution is suspected but cannot be established. Furthermore, the state might not be in breach of its due diligence obligation because it is uncertain whether it has the ability to put an end to the operation. The targeted state's proposed response would otherwise violate, at minimum, the territorial state's sovereignty. Yet, in this situation, the unlawfulness of that response would be precluded so long as the narrow criteria for the plea of necessity are satisfied.

The hostile cyber operation must be grave and imminent before the targeted state may respond. "Grave" denotes a threatened or ongoing hostile operation with consequences that are exceptionally severe, detrimental, or have an otherwise acute impact on an essential interest of the state. A proxy's operation that targets an essential interest with only a limited effect would fall short of this standard. "Imminent" indicates that a targeted state is allowed to respond anticipatorily. Imminence is not to be understood in terms of time. Rather, a threat is imminent where failure to respond would deprive the state of the opportunity to prevent or stop the proxy's hostile cyber operation effectively.[63]

In addition, an essential interest must be affected. Unfortunately, international law does not define the term. The *Tallinn Manual 2.0* experts describe it as an interest "that is of a fundamental and great importance to the State concerned."[64] Certain areas of activity are clearly essential to all states. Paradigmatic examples include national economic well-being, public health and safety, communications, power generation, and national security. Notably, a state's designation of cyberinfrastructure as critical does not definitively mean it qualifies as essential in international law terms.

Moreover, what is essential is a contextual determination. For instance, in all countries, the economic health of the nation is essential. But while tourism drives the nation's economic well-being for some countries, in others it is economically incidental. Accordingly, proxy cyber operations targeting the tourism industry in the former countries might qualify as directed at an essential interest, but not in the latter ones.

A proxy group targeting an essential interest is not enough to warrant otherwise unlawful responses; the additional criteria must be satisfied. Key among these is that the otherwise unlawful operation is the only feasible course of action for putting an end to the grave and imminent peril. If lesser response measures such as acts of retorsion or switching to a secondary or backup system, can safeguard the interest, a targeted state may not act out of necessity.

A state responding in a situation of necessity must be cautious when its response could cause effects on the territory of a state or states from which the proxy's cyber operations either do not originate or to which they cannot be attributed in law. Given the complex and interconnective nature of cyberinfrastructure, these situations present themselves with some frequency. A limiting factor in this regard is that a targeted state must assess whether its response will seriously impair the essential interests of other states.[65] If so, it may not act out of necessity regardless of the magnitude of the harm it is enduring.

Self-Defense

In extreme circumstances, a state may need to respond with use of force level measures to end proxy cyber operations. As noted, countermeasures may not involve the use of force,[66] while whether the plea of necessity allows for a force level response remains unsettled.[67] A state in this situation has three options—consent from the state into which the operations are to be conducted, a UN Security Council resolution authorizing the action, or self-defense. Consent or adoption of a Security Council resolution is unlikely in the case of Russian or Chinese-linked proxy cyber operations, as they would not approve of using cyber force on their territory, and they could use their status as permanent members of the Security Council to veto any resolution authorizing responses at the use of force level. As a consequence, some proxy cyber operations may only be responded to on the basis of the right to self-defense.

Article 51 of the UN Charter, which reflects customary international law, provides "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." That states may use force in self-defense against a cyber armed attack is self-evident. The question is when and how a cyber operation qualifies as an armed attack against which force, whether cyber or kinetic, may be used.

States agree that cyber operations that cause significant physical damage, destruction, death, or injury are armed attacks.[68] Whether those causing a lesser degree of damage or injury, or non-destructive or injurious harm, may be characterized as armed attacks remains an open

debate, but France has gone as far as indicating that a non-destructive cyber operation against its national economy might even qualify.[69] States that have spoken on the issue increasingly agree with the International Court of Justice that whether a non-destructive cyber operation is a use of force at the armed attack depends on its "scale and effects."[70] Precisely where the threshold lies, however, remains unresolved.

The right to act in self-defense is subject to two requirements, necessity and proportionality.[71] Necessity in this context requires a situation in which the targeted state must use cyber or kinetic force to prevent the cyber armed attack, should it be imminent, or to defeat it if the attack is underway. Proportionality limits the degree of force to be used to only that which is required to defeat the imminent or ongoing armed attack effectively.

In the proxy context, two contentious issues loom large. The first is attribution. There is consensus that the targeted state may use force in self-defense against a state or a proxy group if the proxy's cyber armed attack is conducted on behalf of that state or with its "substantial involvement" in the operations.[72] The law is unsettled, however, for situations where a proxy's cyber operation is not attributable to a state either due to insufficient evidence that the operation is being mounted on behalf of the state or because a state's involvement is not substantial. A majority of the *Tallinn Manual 2.0* experts and some states, including the United States, support the view that attribution is not necessary to qualify a proxy cyber operation as an armed attack. A non-attributable cyber operation at the armed attack level also triggers the targeted state's right to respond in self-defense.[73] This is the better position, for if a proxy's operation cannot qualify as an armed attack unless attributable to a state, targeted states would be limited to non-forceful response options—acts of retorsion, countermeasures, or actions out of necessity—to defeat the most severe cyber operations by cyber proxies. In some cases, such a response would prove insufficient.

Assuming that a proxy's cyber operation may qualify as an armed attack without attributing the conduct to a state, controversy also exists around whether a forcible defensive response against the proxy is allowed into a state to which the operation cannot be attributed. A majority of the *Tallinn Manual 2.0* experts support the position, one shared by the United States, that a targeted state may respond with force that is both necessary and proportionate against the proxy so long as the state is unable or unwilling to stop the proxy's cyber armed attack.[74] Take the case of a cyber proxy conducting operations from state A's territory that cause significant damage to state B's critical cyberinfrastructure. The targeted state believes state A is behind the operation but cannot acquire sufficient evidence to attribute the operations confidently. If it cannot be established that state A is able and willing to stop the operations, the targeted state may employ necessary and proportionate cyber operations at the use of force level against the cyber proxy in state A. The same would apply to cyber proxies operating within other states that are not linked to the proxies so long as those other states are unable and unwilling to stop the proxy.

CONCLUSION

The use of cyber proxies by states like Russia, China, North Korea, and Iran adds a layer of complexity to the legal and policy assessments that targeted states must make when considering how to respond to hostile cyber operations. In particular, the factual and legal relationships between a proxy and the state concerned may determine whether particular types of responses against proxy cyber operations are permissible. Nevertheless, in certain circumstances, international law allows for meaningful responses even when attribution to a state is uncertain or altogether missing.

The critical point to grasp is that the international law governing response options is often permissive in terms of allowing responses, but at the same time, can be very nuanced and even unsettled. Thus, every situation merits granular analysis when deciding how to limit, stop, and deter hostile cyber operations by cyber proxies. Over time, state practice in dealing with proxy cyber operations combined with statements from states regarding how they interpret the relevant international law will yield greater clarity on the options available to defeat and deter hostile proxy cyber operations.