

# Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law

---

Dr. Catherine Lotrionte

## INTRODUCTION

In 2012, then-Secretary of Defense Leon Panetta spoke about the rising dangers of a “cyber Pearl Harbor,” analogizing the potential devastation from a cyberattack to that of the surprise attack on the U.S. naval base in Hawaii in December of 1941.<sup>[1]</sup> More recently, U.S. Senator John McCain called the Russian meddling in the 2016 elections “an act of war.”<sup>[2]</sup> The reality of contemporary international relations and the proliferation of cyber operations as an adjunct to both peacetime and wartime operations of states has raised important questions about what would constitute an act of war in the cyber domain, triggering the relevant international legal rules regulating state behavior. As of yet, there is no global consensus about what an act of war carried out by cyber means would look like, versus acts that would fall below the level of an act of war, and although still unlawful, would call for different responses under the law.<sup>[3]</sup>

State actions short of war have been around for a long time. But the current ambiguities in the law related to cyber operations, where details of the international legal principles and rules are poorly defined and subject to competing interpretation or contested application, have left policymakers uncertain about the applicable legal framework for certain actions, and hesitant to respond to those states exploiting the ambiguities as they violate the law with impunity. Furthermore, this lack of clarity in the law creates the potential to misread the intentions of other states that could unnecessarily lead to escalation.

With this in mind, at the outset of this article it is necessary to differentiate between (a) “war” as a figure of speech used for its rhetorical power for political purposes, to heighten the effect of an argument or a news story in the media and (b) “war” as a legal term of art that has special meaning for state conduct under international law.

© 2018 Dr. Catherine Lotrionte



Dr. Catherine Lotrionte is a Brent Scowcroft scholar at the Atlantic Council with the Cyber Statecraft Initiative in the Scowcroft Center for Strategy and Security, and the Founder and former Director of the CyberProject at Georgetown University where she has taught international law and national security law.

Dr. Lotrionte has served as Counsel to the President's Foreign Intelligence Advisory Board at the White House and as Assistant General Counsel at the Central Intelligence Agency. She has a JD from New York University Law School, MA, and Ph.D. from Georgetown University.

While it is accepted that the need to define war is still relevant for some branches of domestic law; for example, in the context of "war powers" in constitutional law and that it is a political question, solely for the determination of those political departments of a government of a state, as to whether a country is or is not engaged in war at any specific time, in so far as contemporary international law is concerned, the definition of war has little bearing on legal analysis. Although there is no one binding definition of war, elements that are common to all proffered definitions under international law, and accepted for purposes of this article, is that war is "a contest between states"<sup>[4]</sup> involving a "comprehensive" use of force.<sup>[5]</sup> In other words, war exists when peace between states has ended, and a certain quantum of hostilities has commenced. While both states and non-state actors implicate the rules related to conflict covered in this article, due to space limitations, this article focuses on state activities and only those actions by non-state actors that are attributable to states.

Rapid technological advances and the changing character of conflict, where threats are less easily defined, attackers can more easily deny responsibility, and the existing ambiguities in the rules are readily exploited by aggressors, has posed new challenges for states in defending their national interests. Today revisionist states actively seek to topple the post-WWII international order, including the rules it is based on, using coercive measures falling below the legal thresholds that traditionally allow for forcible responses.<sup>[6]</sup> By taking advantage of ambiguities in the law they can sow doubt in the lawfulness of responses, eliminating, limiting or delaying responses. In this manner, they are skirting the laws and shifting the international rules, as they try to rewrite them, in their favor. As

evidenced by state practice and government officials' statements,<sup>[7]</sup> these states purposely operate in a gray zone area of conflict, falling between the normal peacetime relations between states, and the state of full-blown overt war or armed conflict.<sup>[8]</sup> For sure, even outside the cyber context, ambiguities and differences about the rules related to use of force have long existed among states. Such gray zone operations, short of armed conflict, have historically manifested in all domains, but in cyberspace adversaries have unparalleled advantages compared to other domains because the rules are even less developed and state practice is still evolving.<sup>[9]</sup> In this respect, the existence of complicated questions about cyber operations related to the international law concerning the use of force is not in itself a new development, it is just about applying some old questions about the law to the newest development in technologies used by states.

Given the different legal consequences that apply depending on whether a state is involved in a war or not, it is important to distinguish between war in the formal legal sense and other kinds of conflicts that fall short of war involving the use of force such as defensive action, reprisal or countermeasure, intervention, or forcible measures not constituting uses of force. The vast majority of hostile cyber operations carried out by states to date fall into the category of actions short of war and, therefore, this article focuses on the challenges of determining what actions by states in cyberspace short of war are prohibited in international law. Certainly, not every hostile act in cyberspace creates a state of armed conflict between nations, but the important question that this article addresses is when, and in what manner, a state can take action through cyberspace or otherwise, in response to hostile cyber operations short of war that threaten the security of the state.

In the context of cyber operations, in recent years governments have affirmed the general applicability of existing international law to states' activity in cyberspace in both peacetime and wartime, recognizing that although there is no global treaty regulating cyber operations, existing treaties, customary rules and general principles of international law<sup>[10]</sup> can be extended to cyber operations through the interpretation of existing sources of law.<sup>[11]</sup> Although existing international laws such as the United Nations Charter (Charter) and the law of armed conflict cannot claim to be directly applicable to cyber operations, given that cyber operations were not even contemplated by those state officials drafting the laws at the time, states have looked to the "spirit" of the existing laws to adapt them to the current threats and new technologies, acknowledging that international law, like the Charter, is a "living, growing" system of rules that are capable of adapting to the needs of the international community through the process of the evolution of customary practice and *opinio juris*.<sup>[12]</sup> These principles are fundamental to the rule of law in cyberspace no less than any other domain.

Today, while there remains little disagreement over whether international law ought to be applied to cyber operations conducted by states, there is much contention over the

precise application and content of many of the specific rules.<sup>[13]</sup> Efforts to clarify and reach agreement on international rules for cyberspace have been ongoing, both inside national governments, in international bodies,<sup>[14]</sup> and through the work of legal scholars,<sup>[15]</sup> but the recent failure in 2017 of the 25 members of the 2016-2017 UN-sponsored Group of Governmental Experts (UN GGE) to reach consensus on the precise manner which the rules apply is a troubling development, and an indication that legal ambiguity persists.<sup>[16]</sup>

As states have yet to clearly define the contours of the law in this space, legal scholars have played an important role in trying to distill some common understanding of the applicable law. In particular, the work of the Group of International Experts who authored the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare (Tallinn Manual 2.0)*<sup>[17]</sup> has usefully contributed to efforts to bring clarity to what the law says about cyber operations and to highlight where the law remains unsettled in this area. Even among the group of experts, there were many issues on which the group failed to achieve consensus, as is reflected in the commentaries of the rules. Although the *Tallinn Manual 2.0* is a non-binding document, such scholarly work has bolstered government efforts to develop the law in this space. In lieu of an international treaty for cyberspace, unlikely to be negotiated in the near future, if ever, it will be for the states to develop the law through the complex, and not always transparent, process of custom. This process will take time as state practice in cyberspace is still at an early stage, not always publicly visible, and state *opinio juris* is limited. This situation raises the importance of efforts by government officials and non-governmental entities to bring more clarity to the international rules that govern aggressive state actions short of “armed attacks.”

This article examines how cyber operations fit within the modern system of international laws related to the use of force, and where circumstances require, how the rules may be adapted and modified to accommodate this new method of conflict, helping to answer the questions: What hostile state activities, short of war, are prohibited in cyberspace, and what measures can states take in response to such hostile cyber operations?

#### MODERN INTERNATIONAL RULES FOR WAR & PEACE

At the start of the 20<sup>TH</sup> century, with the development of more technologically advanced and more lethal weapons, states saw the value of binding agreements limiting the right to resort to armed force. The new rules promoting peace codified in The Hague Conventions of 1899 and 1907,<sup>[18]</sup> however, had little impact in restraining states’ resort to war in 1914. Nor did the Covenant of the League of Nations, adopted in 1919,<sup>[19]</sup> placing restrictions on the resort to war or the 1928 Kellogg-Briand Pact,<sup>[20]</sup> outlawing war as an instrument of national policy, prevent Japanese aggression against China in 1937, the 1935 Italian aggression against Ethiopia, and Nazi aggression that triggered the most destructive war in history.

As states adopted the Geneva Conventions of 1949, a new concept of “armed conflict” was introduced, establishing that the application of humanitarian laws was no longer dependent on the will of states to make formal declarations of war but rather the facts on the ground would determine whether a situation was one of war or peace. Previously, states avoided being bound by the “rules of war” by denying the existence of a state of war. Today, it is a settled norm of international law that a formal declaration of war is not a necessary condition for a state of armed conflict to exist.<sup>[21]</sup> As the legal meaning of “war” lost its relevance, the determination as to when the rules related to conduct in hostilities were triggered would, going forward, be based on an assessment of the intensity and protracted nature of the fighting and the nature of the groups.

According to conclusions of the International Law Association’s Committee on the Use of Force, in their study on the definition of war in international law, an armed conflict exists when there is an intense exchange of fighting by organized armed groups.<sup>[22]</sup> In line with a “first-shot theory,” as soon as the first person is affected by the conflict or the first attack launched, the humanitarian laws of the Geneva Conventions apply.<sup>[23]</sup> Based on this approach, it does not matter where the initial violent act takes place, on the high seas, in outer space or cyberspace, or how the violent act is carried out, air raids, shelling or cyberattacks, its duration or number of casualties, any use of arms by states and organized groups above a *de minimis* threshold will activate an armed conflict and trigger humanitarian laws. Once a state of armed conflict exists, all rules related to how the hostilities should be conducted apply. This fact-based approach to determine when a state of war begins has been widely accepted within international law. Similarly, a proper assessment of when an armed conflict has commenced in cyberspace will depend on the facts of the particular circumstances, and whether the requisite level of hostilities has commenced.<sup>[24]</sup> There has been a general consensus among states that cyber operations carried out during hostilities, as long as those hostilities meet the threshold for armed conflict, will also be covered by the rules of international humanitarian law.<sup>[25]</sup>

### ***The UN Charter Framework***

By the 20<sup>th</sup> century, international law was undergoing a metamorphosis, a revolution concerning inter-state conflict. As the rules concerning the manner in which states would fight their wars were being codified, and new rules negotiated, other rules were established concerning the initiation of armed force during peacetime. The new rules emerged first in the 1928 Kellogg-Briand Pact for Renunciation of War as an Instrument of National Policy in a somewhat restrained fashion, and then, in a sweeping prohibition of the threat or use of force in international relations, in article 2(4) of the Charter.<sup>[26]</sup> In contrast to classical international law in the 19<sup>th</sup> and early 20<sup>th</sup> century, when states had the right to resort to war or initiate hostilities and reprisals to enforce their rights, address an injustice and collect debts owed, and the use of force was the common means to obtain redress and

ensure law enforcement in the international legal order, by 1945, with the drafting of the Charter, the prohibition of the use of force underwent considerable development with a ban on forcible coercion under article 2(4) that clearly outlawed physical coercion, even for the enforcement of legal rights. As proclaimed by the International Court of Justice (ICJ), in 1986, this prohibition on the use of force was reflected in customary international law<sup>[27]</sup> and today is acknowledged, in some respects, as a peremptory rule or rule of *jus cogens*, with widespread acceptance of its applicability to cyber operations conducted by states.<sup>[28]</sup>

#### **Article 2(4) Use of Force Threshold: What's Covered and What's Not**

The Charter's article encompassing the ban on the threat or use of force was drafted in response to the failed attempts of the international community to outlaw and prevent wars. With the intent "to save succeeding generations from the scourge of war,"<sup>[29]</sup> the state officials who drafted the Charter sought to incorporate not only direct armed attacks by states that would lead to war, but also other forms of force below an armed attack threshold as well. The drafters, therefore, avoided the use of the terms "war" or "acts of war" within the article, making the terms obsolete for purposes of the modern international laws related to *jus ad bellum*. On the one hand, the article 2(4) prohibition was intended to "state in the broadest terms an absolute all-inclusive prohibition" on the aggressive use of force between states, prohibiting armed force or the equivalent of armed force.<sup>[30]</sup> On the other hand, there would be minimal uses of armed force that would fall outside of article 2(4), not meant to be covered by the provision.

The article proclaims:

All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.<sup>[31]</sup>

Since its adoption, the article's scope has been clarified through state practice, and *opinio juris*, and ICJ interpretation. In the first instance, the type of force prohibited in article 2(4) is armed force, or the equivalent of armed force, causing violence, as compared to other types of coercive conduct that would not directly cause such violence<sup>[32]</sup> For instance, non-armed force that could include forcible or coercive measures such as economic sanctions, diplomatic protests, psychological operations, and the unconsented presence of official ships and submarines within a state's territory is excluded from the scope of the article.<sup>[33]</sup> These forms of coercion are covered by the principle of intervention in the internal affairs of other states and are not forbidden *per se* but only when they become excessive, targeting an area in which the state has sole discretion to decide freely.

Even within the category of armed force, article 2(4) does not cover all armed force. Armed force of a minimal or *de minimis* amount of force will not be covered under the

article if the acting state has no intention of challenging the state in which it using the minimal force. The role of intent in assessing whether an action is a use of force finds support in ICJ case law as well as state practice.<sup>[34]</sup> The intention in question is not one of motivation for the acts but rather the intention to be considered is that of forcing the will of another state. The intention cannot make an act that violates a rule become consistent with the rule, for example, in the case of arguments in support of interventions for humanitarian purposes. But it can, before any legal determination, affect the determination of the relevant field of law for consideration, for instance, the use of force regime under the Charter versus another legal regime such as international criminal law, international communications law, law of the sea, etc.

Although article 2(4) may not cover minimal forcible actions with confined intent and purposes, depending on the circumstances, such actions may be regulated by other principles of international law such as non-intervention or other treaty-based legal regimes.<sup>[35]</sup> In assessing the applicability of article 2(4) in various circumstances, the gravity of the force is relevant as well as the intent of the state to use force against another state.<sup>[36]</sup> If the force used is not excessive and the state acting does not intend to use force against the state, the actions may not be covered by the prohibition in article 2(4). For example, if a state through cyber means interrupts the operations of a command and control server within another country without its consent in order to stop cyber intrusions against the acting state's banks for instance, because the force was minimal and not intended to force the will of the other state, it may be considered not to constitute the type of force that article 2(4) was meant to cover. Likely to be excluded from the scope of article 2(4) would be the disruption of Internet service by denial of service attacks. These cyber actions will not as a general matter fall within article 2(4). If these actions are characterized as unlawful, it would likely be so not in respect to article 2(4) but more generally of the principle of state sovereignty, the norm of non-intervention or other bodies of law relevant to the context of the situation.

States have agreed that cyber operations can violate article 2(4) of the Charter, the principle of non-intervention under customary international law and other *lex specialis* rules, however, there remains a debate as to whether cyber operations that do not violate these laws may still violate the customary legal principle of sovereignty in carrying out cyber operations within the territory of another state without its consent. Although a review of this issue is beyond the scope of this article, it is worthy of brief mention to highlight what seems to be an area of disagreement and unsettled law. The basic legal question is what types of actions would be covered by the principle of sovereignty under international law as applicable to cyber operations. There are conflicting views among scholars on this issue<sup>[37]</sup> with government officials recently weighing in on this debate, providing some valuable insight into how the law may be developing on this issue. In May 2018, the United Kingdom (UK) Attorney General, speaking for the first time in such detail, set out the UK's

legal position on some specific international rules for cyber operations, to include the principle of sovereignty, and highlighting areas of disagreement with previous interpretations of the rules for state responsibility. Related to the issue of sovereignty, the Attorney General rejected any cyber-specific rule related to the “violation of territorial sovereignty” from cyber operations that cause “interference in the computer networks of another state without its consent” that fall below the threshold for a violation of the rule of non-intervention.<sup>[38]</sup>

Taken together with prior statements by US government officials, generally in line with the UK statement although less detailed, these statements would indicate that some states are interpreting the rule of sovereignty as one that would not necessarily cover cyber operations causing minimal impact on another state’s infrastructure as long as they do not trigger the prohibition on the use of force, the norm of non-intervention or any other existing treaty obligation. Under this approach, examples of cyber operations not implicating the sovereignty rule could include implanting of malware on another state’s infrastructure and interruption of Internet service through a denial of service attack, among other possibilities. Given the historical practice of states acceptance, albeit in a seemingly reluctant manner at times, of activities of foreign governments within their territory without their consent, the UK approach seems to make the most sense. After all, it has not been the case in state practice that mere minor intrusions into territorial property with limited impact on the state would constitute an internationally wrongful act. Had this been so, the reality of the day-to-day activities of intelligence agencies would be dramatically different.

The apparent acceptance, at least by the UK, of a minimal effects test for the rule of sovereignty in cyberspace is in line with a minimal effects or gravity test for uses of force as outlined in this article, and may be most relevant to cyber operations that persist at a low level of intensity. This approach for assessing what constitutes a use of force, although of debate by some legal analysts, is gaining acceptance with support found both in state practice and the implications of ICJ decisions where not all forcible measures that contain a foreign element have been found to constitute a prohibition of article 2(4).<sup>[39]</sup> In such instances the focus has been on the assessment of the gravity of the action and the intention of the actor, or purpose of the action.<sup>[40]</sup> In one of its earliest cases, the *Corfu Channel*, the ICJ indicated that minimal uses of force not used “for the purpose of exercising political pressure” on another state would not constitute a use of force under article 2(4).<sup>[41]</sup> Although the Court ruled that the UK’s minesweeping operations in Albania’s territorial sea violated its sovereignty and used the phrase, a “manifestation of a policy of force” in describing the British actions, the Court did not conclude that such action violated article 2(4).<sup>[42]</sup> In a number of other situations, in enforcement cases involving maritime enforcement, law enforcement actions involving the arrest of someone in another state’s territory without authorization, environmental protection acts, hostage rescue operations, and the interception of foreign aircraft that has entered a state’s airspace without permission, the minimal armed

force that was used was found not to be covered by the regime on the use of force under article 2(4) but rather by other areas of international law.<sup>[43]</sup> State practice has confirmed that such actions convened as enforcement measures by states, limited in scope and intensity, with no intention to use force against the other state, do not come under article 2(4) but rather other specific rules relevant to the case at issue.<sup>[44]</sup>

A central question for cyber operations, and the primary focus of this article, of whether a hostile cyber operation by a state is an article 2(4) use of force violation, an unlawful intervention or an armed attack, is critical to the determination of what responses would be legal under international law. Even though the intent of the framers seemed clear in drafting article 2(4) that certain coercive measures would not be covered, and the long practice of states under the Charter has demonstrated support for that intent, without a precise definition of the term “use of force” within the treaty, practitioners and scholars continue to disagree over the meaning of the term “use of force.” They have struggled to establish a single approach for distinguishing those actions by states that would fall within the article 2(4) regime versus those that would fall under different legal regimes, and for those actions that do fall under the regime of the use of force, which actions would fall below the article 2(4) threshold and which ones would surpass the threshold.<sup>[45]</sup> In the context of cyber operations, there remains much contention over the specific cyber operations that would violate article 2(4), fall outside the scope of the article, fall below the threshold of the article, or surpass the threshold and reach the level of an armed attack. What is of general agreement in the context of cyber operations is that for such operations to constitute a use of force under international law they must be attributable to a state, reach the gravity threshold for the use of force as meant by article 2(4), and must be exercised in the context of “international relations” between states.<sup>[46]</sup> For those cyber operations that meet these requirements and are regulated by the Charter regime, they constitute a use of force, and therefore there must exist a “proper legal basis” for them in order not to violate the prohibition within article 2(4).<sup>[47]</sup>

Historically, in trying to delineate clear lines of distinction under the law between state actions that would constitute uses of force versus other actions, international legal scholars disagreed over the appropriate focus for assessing the legality of such actions. The different proposals involved focusing on the instruments or weapons used, the characteristics of the targets, the intent of the attackers or the effects generated by the actions.<sup>[48]</sup> Ultimately, the dominant approach that has been accepted, for cyber operations as well, is one based on the effects of the actions.<sup>[49]</sup> In line with an effects-based approach, kinetic operations that have a direct destructive impact on property or injurious effects on persons, beyond a *de minimis* effect and under circumstances where the regime of use of force is applicable, would constitute armed “uses of force” and, therefore, illegal under article 2(4). Analogously, under an equivalence approach for cyber operations, states have

assessed that cyber operations that cause or are reasonably likely to cause similar damaging consequences or effects as those produced by kinetic weapons, with physical damage to persons or property, excluding those actions of *de minimis* effects not covered by the article 2(4) use of force regime, would be a use of armed force action prohibited by article 2(4).<sup>[50]</sup>

While it is virtually uncontested that cyber operations, which cause or are reasonably likely to cause physical damage, loss of life or injury to persons would fall under the prohibition contained in article 2(4) under this equivalence test, the question remains how to characterize cyber operations that produce damaging consequences but no physical destruction. In other words, is there a minimum threshold of gravity that the consequences of a cyber operation must reach to be a violation of article 2(4) versus, for example, the norm of non-intervention?<sup>[51]</sup>

For those cyber operations that are disruptive, interrupting the functionality of a target, but failing to cause lasting physical damage, a strict effects-based equivalence test under the law raises questions as to whether such attacks would constitute a “use of force” under article 2(4).<sup>[52]</sup> Such a narrow approach based on kinetic effects fails to take into account the dependency of modern society on the functioning of computer networks. It is now possible for critical infrastructure to be compromised, and society crippled without destroying the computer networks themselves. Government officials have raised concerns about the devastation that would occur if such critical infrastructure were disabled by a cyberattack, causing cascading effects between sectors and second and third-order effects disrupting societal, economic, and governmental functions.<sup>[53]</sup> The question remains then today, for cyber operations against those physical or virtual systems and assets of a state, the disruption of which would render them ineffective or unusable causing devastation to a state’s security, economy, public health and safety, and environment, would they constitute uses of force in violation of article 2(4) or even an armed attack?

There exists little doubt that as a practical matter a state targeted by a cyber operation that shuts down its electric grid, leaving millions without power, disrupting the financial markets and government communications, though without causing immediate physical damage, would be considered a “use of force,” if not an “armed attack.”<sup>[54]</sup> And yet, under an effects-based equivalence approach, such attacks would not constitute uses of force against the state without some level of physical damage.<sup>[55]</sup> On the other hand, a more flexible interpretation of article 2(4), one based on the intent and logic of the Charter provision, the ruling in the *Nicaragua* case,<sup>[56]</sup> and a broader meaning of a “use of force” for cyber operations specifically targeting critical infrastructure may be gaining support from international legal experts and governments.<sup>[57]</sup> Such an approach would more effectively address the potential for devastating effects from cyberattacks against critical infrastructure and could encompass cases of cyber operations that significantly disrupted,

for extended periods of time, the functionality of critical infrastructure causing significant negative consequences, albeit no physical damage, to the national security and welfare of the state and citizens. The requisite level of disruption would have to go beyond mere inconvenience and “significantly disrupt the functioning of critical infrastructure,” versus solely non-critical infrastructure, to fall within the scope of article 2(4).<sup>[58]</sup> This approach, in line with the decision in *Nicaragua*, although not providing the injured state with a right of self-defense, does provide it with recourse to other measures under international law that will be discussed later in this article.<sup>[59]</sup>

### ***Below Article 2(4) Use of Force Threshold: Getting to the Gravity Question***

The Charter framers recognized that aside from using armed force, states also employed other non-forcible but coercive measures in their international relations with other states to influence them. The *travaux préparatoires* of the Charter reveal that the drafters made a conscious decision not to include these other non-armed, non-violent coercive measures within the Charter prohibition on the use of force in article 2(4).<sup>[60]</sup> Coercive non-armed measures, such as economic or psychological coercion and political pressures, were purposely left outside the Charter framework.<sup>[61]</sup> Rather, these activities would either be covered under a customary international legal principle such as non-intervention<sup>[62]</sup> or be left unregulated by the law. As distinguished from uses of force that violate article 2(4), violations of a state’s territorial integrity and the principle of non-intervention can occur “with or without armed force.”<sup>[63]</sup> In short, the type of force prohibited by article 2(4) is armed force or the equivalent of armed force, in contrast to other types of forceful coercive conduct.

In addition to the non-armed coercive measures that fall outside of article 2(4), like economic sanctions, there are additional measures that might be “armed” or involving some minimum form of physical force, but would fail to constitute a use of force for purposes of article 2(4) because they do not meet a minimum threshold of gravity.<sup>[64]</sup> In other words, they are minimal uses of armed force that article 2(4) was not meant to cover. This methodology of using a gravity test to distinguish different levels of force for assessing article 2(4) violations is based on the same methodology used in the *Nicaragua* case to distinguish article 2(4) uses of force from armed attacks under article 51, analyzing the scope, intensity, and duration of the action. The reasoning behind using this same methodology to determine the article 2(4) threshold for uses of force and distinguishing article 2(4) uses of force from other actions, although possibly illegal, falling outside of article 2(4) is three-fold: firstly, such minor uses of force that serve limited intentions and purposes are not equivalent to the purposes of those uses of force as intended to be outlawed by article 2(4), secondly, these minor uses of force do not implicate the “international relations” between states that article 2(4) explicitly incorporated into its language, and thirdly, these uses of force have a lesser level of intensity that falls below the threshold of a use of force that was intended by article 2(4) of the Charter.<sup>[65]</sup>

This approach for uses of force “appears to be gaining ground in legal doctrine”<sup>[66]</sup> based on state practice, the implications from ICJ decisions, and commentary by scholars and state officials.<sup>[67]</sup> According to the Independent International Fact-Finding Mission on the Conflict in Georgia, the “prohibition of the use of force covers all physical force which surpasses a minimum threshold of intensity” and “[o]nly very small incidents lie below this threshold, for instance, the targeted killing of single individuals, forcible abductions of individual persons, or the interception of a single aircraft.”<sup>[68]</sup> In the cases of actions such as police or security operations where the force used is of a low intensity, not intended to force the state to do or not do something against its will, not engaging the relations between states, they have been characterized as falling outside the coverage of article 2(4). Such operations have included: individual international abductions, extraterritorial criminal enforcement measures, “hot pursuit” against criminals on land, enforcement actions at sea, neutralization or interception of aircraft entering a state’s airspace without authorization, rescuing nationals abroad, small-scale counterterrorism operations abroad, to the targeted assassinations carried out by secret services in another state, “where the coercive character of the operation within the foreign territory is very limited” and is not targeted against the state.<sup>[69]</sup>

Outside of the cyber context, the recent case of Russia’s poisoning of a former Russian spy in the UK provides insight into how states categorize various actions under the law, in accordance with the minimal threshold approach to uses of force. In her initial statement to Parliament on the matter, British Prime Minister Theresa May forewarned that unless Russia responded to the UK’s accusations that Russia had used a military-grade nerve agent to kill someone on British soil, May stated, “we will conclude that the action amounts to an unlawful use of force by the Russian State against the United Kingdom.”<sup>[70]</sup> In her statement, the Prime Minister never invoked the Charter or article 2(4) explicitly, although referring to an “unlawful use of force.” Notably, however, in the joint statement on the matter released by the UK, the US, Germany, and France, a few days after May’s initial statement, the four countries described Russia’s action as “an assault on UK sovereignty and any such use by a state party is a clear violation of the chemical weapons convention and a breach of international law.”<sup>[71]</sup> In that statement, there was no mention of a use of force or article 2(4) of the Charter. Rather than assessing Russia’s actions under the use of force regime, the UK, US, Germany, and France treated the poisoning of a foreigner on UK soil as a violation of the United Kingdom’s sovereignty and a breach of the rules related to the use of chemical weapons. This incident, and the states’ responses to it, suggest support for the approach discussed in this article for assessing the legality of different uses of force.

In other historical incidents of states using limited armed force, the states involved have also failed to invoke article 2(4) of the Charter. As an illustration, the forcible abduction

of Adolf Eichmann from Argentina in 1960 by Israeli intelligence was found by the UN Security Council to be a violation of Argentina's sovereignty. The Argentina delegate to the UN never invoked article 2(4) nor did the Security Council in its resolution.<sup>[72]</sup> In contrast, the abduction of General Noriega in Panama in 1989 following the US invasion, was considered in the context of the gravity of a military invasion of another state and not the individual abduction of one person. In short, a forcible abduction may or may not constitute a use of force depending on the full context of the case and the gravity of the force used.<sup>[73]</sup> For these kinds of forcible enforcement measures that are not covered by article 2(4), and therefore do not constitute an unlawful use of force, they may still constitute violations of other legal obligations, such as the obligation not to intervene in the affairs of another state or breaches of other specific treaties.<sup>[74]</sup> These minor armed uses of force fall outside the scope of article 2(4), based on the context and domain in which they occur and their gravity, and while potentially implicating other regimes of law (international criminal law, sea and air law) they would not violate the Charter.

Applied in the cyber context, according to this "minimum use of force" standard for the use of force, a "cyber operation that causes minimal damage in another state's territory such as the destruction of a single computer or server," with no hostile intent towards the state itself, and without further effects, "would clearly not fall within the scope of the provisions" of article 2(4) under the minimum use of force test.<sup>[75]</sup> In applying the *de minimis* standard, the quantity of force matters as well as the context of the incident. Such an operation that involves the destruction of property in another state, would, however, impose effects within another state's territory and, if coercive, in the sense of intended to compel a state to behave in a manner other than how it would normally behave, be an unlawful intervention.<sup>[76]</sup> According to the then-legal advisor to the U.S. Department of State, Harold Koh, in discussing some of the factors that would be relevant to a legal assessment of actions involving uses of force in cyberspace, he specifically included "intent" and gravity, among others, to be taken into consideration.<sup>[77]</sup> Ultimately, whether a minimum use of force will constitute a violation of article 2(4) will depend on the specific circumstances of each case.

Analyzing the meaning of a "use of force" in this more limited manner affords a state subject to a use of force in violation of article 2(4) more options for legally responding than the state would have under an approach accepting a broader meaning of a use of force under article 2(4). Under a broad interpretation of article 2(4) uses of force, and a broad interpretation of the *Nicaragua* Court's findings, to be discussed in more detail in the next two sections, a victim state would be prohibited from using forcible responses unless the attack against the state rose to the high threshold of an armed attack. In contrast, with a limited interpretation of article 2(4), states that are targets of uses of force violating article 2(4) but not constituting an armed attack under article 51 of the Charter can conduct forcible responses as long as such responses are of a *de minimis* nature or gravity both in its objectives and its means. Such forcible responses would fall outside of the

article 2(4) prohibition and would constitute permissible countermeasure<sup>[78]</sup> even though they may cause minor physical harm, injury or damage in the state's territory.<sup>[79]</sup>

An example of a cyber operation that would not necessarily be covered by article 2(4) could include the disruption of Internet service that, although possibly involving the violation of certain economic rights or property rights under international law, would not be covered by article 2(4) based on the gravity of the effects and the full context of the situation. Other actions not covered by article 2(4) could include, for instance, the interruption of the production lines of a manufacturing company in another state through Internet-facing network connections that would involve hacking into the manufacturing control units and robotics and potentially causing them to produce faulty manufacturing or physically destroying the manufacturing equipment itself. Although likely to violate other laws such as international criminal law, depending on the context and gravity of effects, they may not be covered by article 2(4) and therefore could constitute lawful countermeasures if done in response to a wrongful act and complying with the other requirements for countermeasures such as proportionality that will be discussed below in more detail.<sup>[80]</sup> In contrast, if a broader interpretation of article 2(4) is accepted, expanding article 2(4) to include all uses of force, any proportionate forcible response, even in-kind, to a use of force would be in violation of article 2(4) and a prohibited forcible countermeasure.

#### ***Article 51 Self-Defense Exception to the Prohibition on the Use of Force***

Under the Charter, the article 2(4) prohibition on the use of force was subjected to two explicit exceptions: military action authorized by the UN Security Council following a determination of 1) the existence of a threat to the peace, a breach of the peace, or 2) an act of aggression, and self-defense in response to an armed attack. As an exception to this prohibition, states may use force if the UN Security Council authorizes it pursuant to its responsibility to maintain peace and security; this includes the authority to respond to threats to the peace, breaches of the peace, and acts of aggression.<sup>[81]</sup>

The article proclaims:

Nothing 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.<sup>[82]</sup>

As a matter of customary law, a state can also use force in self-defense if an armed attack is imminent but has not yet occurred.<sup>[83]</sup> The article 51 principle of self-defense reflects customary international law and has been recognized by states as applying to defense against cyberattacks that are equivalent to armed attacks under article 51.<sup>[84]</sup>

As an exception to the prohibition on the use of force, a state can employ forcible cyber operations in response to an armed attack that has occurred or is imminent<sup>[85]</sup> as long as the forcible defensive measure targets the responsible state or non-state actors<sup>[86]</sup> and

complies with the customary legal principles of proportionality and necessity, as discussed later in more detail.

### ***Distinguishing an Article 51 Armed Attack From an Article 2(4) Use of Force***

Interpreting the rule of self-defense for cyber within article 51 requires an understanding of the meaning of the term “armed attack,” that, like the term “force” as used in article 2(4), remains undefined in the law. The ICJ in the *Nicaragua* case, without providing a specific definition for an armed attack or use of force, drew a distinction between the two terms and developed a “gap” theory, where only the most severe or grave uses of force would constitute an armed attack, utilizing a “scale and effects” standard to distinguish between a use of force and the gravest uses of force that would constitute armed attacks.<sup>[87]</sup> In other words, a certain degree of armed force could meet the gravity threshold of article 2(4), nonetheless fail to trigger the higher threshold for article 51 self-defense if the armed force was not sufficient enough.

Based on this “scale and effects” test utilized in the *Nicaragua* case, isolated or minor incidences that do not threaten the safety of the state, while hostile and unlawful, would not constitute an armed attack reference to the Charter’s right of self-defense. If, however, the results of the armed force met the gravity threshold, resulting in or imminently resulting in a considerable loss of life or extensive destruction of property, it would constitute an armed attack under international law, triggering the victim state’s right to use lethal force in response. There is a minority view among some states and legal experts, including the US, that there is no distinction between a use of force and an armed attack, and that any unlawful use of force qualifies as an armed attack triggering the right of self-defense. The US has taken this position with respect to cyber operations as well.<sup>[88]</sup> While disagreements persist between states and commentators as to the validity of a gap between the thresholds and the nature of any gap that may exist, state practice has supported the position that kinetic operations causing significant physical damage, injury or death would qualify as a grave use of force and therefore an armed attack; this reasoning has been extended to cyber operations.<sup>[89]</sup>

Since *Nicaragua*, government officials and scholars have struggled to define the precise threshold at which a use of force would constitute an armed attack, finding “[I]t is almost impossible to fix the threshold of force employed to define the notion of armed attack,” and failing to develop a bright-line test.<sup>[90]</sup> Disagreement continues to exist as to whether the 2010 Stuxnet operation against the Iranian nuclear program that damaged over 1000 centrifuges, qualified as an armed attack.<sup>[91]</sup> In accordance with *Nicaragua*, a use of force would constitute an “armed attack” only when both the *scale* and the *effects* of the use of force were grave enough. For the sufficient *scale* to be met under this test, considerable magnitude and intensity must be involved, taking into consideration the amount of force used and duration of the attack. For the threshold of *effects* to be met, the consequences

have to involve substantial destruction to important elements of a state, namely, its people, territory and, in certain cases, its economy that compose the security of the state. Even in cases where armed force is used and causes damage, unless it is of a high enough intensity, it will not constitute an armed attack. In finding that mere “frontier incidents” using military force do not have the necessary gravity to be considered armed attacks, the ICJ supported this position.<sup>[92]</sup>

This aspect of the Court’s decision has faced much criticism in that the gap created by the Court between permissible self-defense and lower level attacks by armed bands served to reduce the barrier to armed aggression because it took away the military deterrent from lawful recourse to self-defense.<sup>[93]</sup> The decision was further criticized for not elaborating on the required scale and effects necessary to reach the threshold of an armed attack nor what type of response might be appropriate for acts that fall below the threshold. In its opinion, the Court indicated that the threshold of gravity is a flexible one dependent on the specific circumstances of each case. For example, in contrast to the example of “frontier incidents” in the *Nicaragua* case, in accordance with the same scale and effects standard developed by the Court in another case with a different set of facts, the Court “[did] not exclude the possibility that the mining of a single military vessel might be sufficient to trigger the ‘inherent right of self-defence.’”<sup>[94]</sup> Therefore, even a single incident of armed force that leads to a considerable loss of life and extensive destruction of property would be of sufficient gravity to constitute an armed attack.<sup>[95]</sup> In the context of cyberspace, a single cyber operation against computer systems that caused a significant number of fatalities would likely constitute an “armed attack.”<sup>[96]</sup>

For cyber operations that do not result in direct physical damage but result in destructive second-order effect, there is growing support based on the stated opinions of governments that such actions may constitute not only uses of force but also armed attacks under the Charter framework.<sup>[97]</sup> As states have come to recognize the vulnerabilities of critical infrastructure to cyberattacks that could inflict substantial destruction to critical elements of a target state (its people, economy, and security infrastructure) international jurists and governments have concluded that disruptive cyberattacks against such infrastructure, although not causing direct physical damage to the infrastructure, nevertheless of the requisite magnitude resulting in significant damage to the nation or its people, versus mere inconvenience, could constitute an “armed attack,” triggering the legal right to use forcible responses in self-defense.<sup>[98]</sup> For example, a cyber operation that interrupts the cooling functionality of a nuclear reactor, while not destroying the reactor causes the cooling system to malfunction, leading to the release of radioactive materials and the loss of life, would result in significant enough second-order effects that amount to an armed attack irrespective of the fact that the initial cyber operation did not produce direct harmful or permanent effects to the reactor.<sup>[99]</sup> In cases of cyber operations that cause no

physical damage but severely incapacitate critical infrastructure, such as banking institutions, if the effects are serious enough, may constitute an “armed attack.”<sup>[100]</sup>

In line with the “scale and effects” approach, only armed attacks will trigger the right of self-defense and therefore all other attacks or hostile actions by states that fall below this threshold are classified as uses of force, interventions or general violations of sovereignty, depriving the target state of such attacks the right of forcible self-defense under article 51. This standard of scale and effects, however, is a “variable standard”<sup>[101]</sup> which does not require it being applied separately to each hostile act, but instead can be applied in combination with multiple acts to meet the high threshold of an armed attack. The Court has implicitly accepted this approach, the doctrine of “accumulation of events,” in particular circumstances where consecutive attacks take place that are linked in time, source and cause, and are part of a “continuous, overall plan of attack purposely relying on numerous small raids.”<sup>[102]</sup> In such cases where there may be some small-scale uses of force falling below the level of an armed attack, collectively they can amount to such an armed attack. In this context, cyber operations against a state that would in themselves merely constitute “less grave uses of force,” when forming part of a chain of events carried out by the same source, can qualitatively transform into an “armed attack” triggering the right of self-defense.<sup>[103]</sup> The question remains, however, as with assessing the gravity threshold for singular armed attacks, how many individual lesser grave uses of force are required to constitute an armed attack?

Given that the most common form of cyber force between states has been a stream of low-intensity cyber operations versus actions at the armed attack level, this doctrine of accumulation of events in the context of self-defense may be relevant.<sup>[104]</sup> Under this doctrine, in circumstances where there are a number of “less grave uses of force” that take place either exclusively in the cyber domain or different domains (cyber and kinetic) that can be linked together to form part of a chain of events by the same state, the nature of the acts taken together could amount to an “armed attack,” triggering the right of self-defense.

### ***Self-Defense Responses to an Article 51 Armed Attack***

The right of individual or collective self-defense referenced in article 51 of the Charter is the right of a victim state to use offensive force against a state legally responsible for an armed attack to prevent or stop harm to the state or its allies.<sup>[105]</sup> All self-defensive actions, to include cyber operations carried out in self-defense, must be proportionate and necessary. Necessary responses in self-defense are those actions that are used as the last resort and have been determined to be the only means by which to repel an attack or prevent a subsequent attack.<sup>[106]</sup> Proportionate responses are those that are in balance against the purpose of repelling the attack to end the situation or threat, which caused the attack.<sup>[107]</sup> Proportionate self-defense responses can be quantitatively greater than the initial armed attack since it aims to repel that attack.<sup>[108]</sup> In other words, if the threat continues after an

initial armed attack, the victim state can use all necessary force to eliminate the threat. Beyond just intercepting the immediate armed force, the victim state could use deadly force to degrade the attacker's military capabilities or seize territory in order to assure its future security against the attacker, imposing a higher level of cost to the adversary than the initial attack imposed, so long as it has been determined that such a level of force is required to stop the threat.<sup>[109]</sup> What matters in assessing the proportionality of a self-defensive action then is "the result to be achieved by the defensive action and not the forms, substance, and strength of the action itself."<sup>[110]</sup> The right of self-defense has been recognized to extend to cyber operations that rise to the level of an armed attack.<sup>[111]</sup> If forcible cyber operations meet these standards for self-defense they would be lawful.

In determining an appropriate legal self-defense response, attribution is key. It does not matter where an armed attack occurred,<sup>[112]</sup> what type of weapon was used to carry out the attack,<sup>[113]</sup> whether the target was civilian or military, or how many individual incidents occurred.<sup>[114]</sup> As long as the victim state can identify the responsible state for the attack and the overall effects of the incident or incidences reach the high threshold for an armed attack, the victim state can act in self-defense against the responsible state. For example, if a state carries out an attack, whether by a kinetic or cyber operation, against a civilian computer system owned and operated by a private company within the territory of another state that causes a devastating impact, although it has no connection to military or government entities, such an attack will constitute an armed attack for purposes of article 51.<sup>[115]</sup> Neither the nature of the attack as a cyber operation nor the governmental or private nature of the target is relevant to the determination of the existence of an armed attack against the state in its territory.<sup>[116]</sup> In responding to an armed attack, actions are not limited to in-kind methods; for instance, reactions to cyberattacks that constitute armed attacks could be exercised by physical, cyber, or other means.<sup>[117]</sup> Furthermore, there is no requirement under international law for states to publicly disclose the basis for its attribution assessments.<sup>[118]</sup>

### ***Defensive Self-Help Responses to Hostile Actions Below the Threshold of Armed Attack***

Historically, defensive self-help involved retaliatory measures by a state against another state that had violated its rights protected by international law. The idea of such measures was based on a lack of centralized enforcement in the international community and, therefore, self-help measures played an important role in bringing about a situation that conformed to the law. The recognized value of such measures "lay in the possibility of gaining redress without creating a formal state of war."<sup>[119]</sup> With the modern development of international law within the Charter, article 51 established forcible self-defense as a separate institution from self-help, making armed force in self-help mostly forbidden except for the occasional resort to *de minimis* forms of force due to the ineffectiveness of the UN Security Council to enforce the law.<sup>[120]</sup> Under the old concept of self-help and the right of states

to wage war, a state's recourse was practically without limitation and covered retorsions, reprisals, both armed and peaceful, peaceful blockade, intervention, and even war. Today, self-help still includes retorsions, countermeasures, and necessity, which are all remaining legal options for states to act unilaterally for coercive enforcement of rights, albeit with a number of restrictions.

As international law provides states with options for responses to hostile actions below the article 51 threshold in the physical domain, so too does the law permit victim states to respond to unlawful actions that fall below the armed attack threshold. Especially in an era where states are pursuing their strategic objectives and coercively operating in the gray zone, victim states will find relief as international law does not leave such states powerless to defend against and respond to such gray zone cyber threats. As recently expressed by the then-nominee for Commander, U.S. Cyber Command, "Although cyber operations not involving loss of life or significant destruction of property may not constitute an armed attack those operations causing significant impact on U.S. foreign and economic policy interests may nonetheless violate international law and trigger U.S. response options."<sup>[121]</sup> Indeed, customary law has provided multiple options for victim states to respond to offensive measures by other states, short of war or an armed attack, whether the measures are conducted in cyber or not.

For those states that are victims of coercive or forcible cyber operations that fall short of an "armed attack" in article 51, recourse can be taken unilaterally, to include the adoption of retorsions and countermeasures and measures invoked under a plea of necessity that do not reach the "armed attack" threshold.<sup>[122]</sup> According to the *Articles of State Responsibility* (Articles) drafted by the UN International Law Commission (ILC),<sup>[123]</sup> countermeasures and actions of necessity are measures that would otherwise not be justified under the law but for, in the case of countermeasures, a prior wrongful act against the state, and in the case of acts of necessity, exigent circumstances where the state's essential interest are in "grave and imminent peril."<sup>[124]</sup>

Given the role that the Articles will play in assessing state responsibility for cyber activities, some background on the Articles is relevant. In 2001 over forty years of work of the ILC on state responsibility was concluded with the adoption of fifty-five draft articles. Unlike the ILC's previous projects, the work did not result in a treaty but rather in draft articles that were "taken note of" by the UN General Assembly, indicating the challenges with reaching agreement on the Articles during the drafting process and concluding without universal state agreement. Although the Articles are not a binding source of law, they can serve as a source of ascertaining the law, similar to the writings of highly qualified publicists, and indeed, some aspects of them have been accepted as customary law by international tribunals and at least some state practice has provided evidence of its customary characteristic.<sup>[125]</sup> Some provisions of the Articles, however, were controversial

during the drafting and still are, particularly the articles on countermeasures, leaving the status of those provisions under the law uncertain as they have not been accepted by states as authoritative restatements of customary international law.<sup>[126]</sup> Related to the work of assessing the legality of cyber operations, the *Tallinn Manual 2.0* relied heavily on the Articles in developing some of its rules. Given the lack of clarity and controversy over some provisions of the Articles, it may be that with respect to the Tallinn Manual's rules that are based on these same provisions, more work will need to be done by states and possibly judges before the law is clear in this complex area.

For assessing state responsibility, as the Articles did, it is useful to first distinguish countermeasures (previously called reprisals)<sup>[127]</sup> and pleas of necessity from retorsions under international law. An act of retorsion is a coercive, politically unfriendly, but lawful act, not involving any breach of international obligations owed to the target state, whether treaty-based or customary and thereby do not require any legal justification.<sup>[128]</sup> States can undertake cyber or non-cyber retorsions at any time to influence another state's actions, regardless of whether there was a prior law violated or any detrimental effects to the interests of the targeted state from the retorsions.<sup>[129]</sup> Although retorsions can be taken at any time and have few, if any, restrictions because of their legality, typically, they are taken in response to a breach of an international legal obligation owed to the state. Common examples of retorsions include protests and verbal condemnation or diplomatic demarches, discontinuing development aid, denying entry visas, declaring that a diplomat is *persona non grata*, imposing travel restrictions on foreign nationals within the state, terminating cultural and educational exchanges, and imposing unilateral sanctions.<sup>[130]</sup>

Recent examples of retorsions conducted by the US in response to cyberattacks have included unilateral sanctions against North Korea in response to the Sony cyberattack<sup>[131]</sup> and against Russia in response to its cyber operations against the Democratic National Committee and related interference with the 2016 US election.<sup>[132]</sup> In addition to sanctions, the US expelled Russian diplomats from US territory, also constituting a retorsion.<sup>[133]</sup> These US actions were lawful, although considered unfriendly, and could have been done irrespective of the unlawfulness of the cyber operations conducted by North Korea and Russia.<sup>[134]</sup> An example of a *cyber* retorsion would be a state selectively blocking, at its own gateway, another state's Internet traffic from entering the territory, provided such action did not violate any existing treaty agreement between the states or any customary law.<sup>[135]</sup>

In contrast to retorsions, countermeasures are actions, short of armed attack, or omissions that breach an international obligation owed the targeted state and therefore are unlawful except for a prior law violation by the targeted state.<sup>[136]</sup> The purpose of countermeasures is to compel the responsible state to comply with its international obligations owed to the injured state and make reparations for the injury caused.<sup>[137]</sup> While countermeasures have been established through international practice and decisions from

tribunals and courts as a circumstance precluding wrongfulness, the legal regime applicable to countermeasures is far from well-established as states have objected even during the drafting of the *Articles of State Responsibility* to different aspects of the Articles as they apply to countermeasures in particular. In the comments the US submitted to the ILC during the drafting process emphasis was placed on the US objections to the restrictions on the use of countermeasures that were included in the Articles.<sup>[138]</sup> This may indicate that for certain aspects of the regime of countermeasures, the Articles, and potentially the rules on countermeasures in the *Tallinn Manual 2.0*, are more a progressive development of the law, rather than the codification of existing customary rules. Indeed, the topic of countermeasures was one of the contentious issues in the discussions of the 2017 UN GGE that failed to reach a consensus report.<sup>[139]</sup>

According to the *Articles of Responsibility*, an injured state that has suffered a wrongful act by another state may commit a wrong in reaction, a countermeasure, as long as it is “commensurate” with the injury suffered from the initial wrongful act, taking into consideration the rights in question<sup>[140]</sup> and the state’s response is aimed at inducing an end to the initial wrong, and the provision of damages for injuries suffered.<sup>[141]</sup> Despite the clear nature of the requirement of a prior wrongful act, there remain some unresolved issues related to this requirement for countermeasures. For example, due to a lack of state practice and no treaty-based clarification, the specific issue of whether a state that conducts countermeasures must be directly injured is of great debate with opposing views.<sup>[142]</sup> The question being, does the state that is conducting the countermeasure have to be the state that suffered the injury from the wrongful act. This issue of individually or collectively conducted countermeasures, irrespective of individual injury, in defense of another injured state or in respect of breaches of obligations *erga omnes*, has yet to be resolved, leaving open the further development of the law through state practice and *opinio juris* and the possibility for collective, or third-party, cyber countermeasures.<sup>[143]</sup>

Another contentious issue that remains unsettled is whether a state can conduct forcible proportionate countermeasures that would violate article 2(4) of the Charter in response to forcible actions that are below the article 51 armed attack level of the Charter.<sup>[144]</sup> While there is widespread agreement that countermeasures must not be of the severity of an armed attack as meant by article 51 of the Charter, the debate remains over the allowable level of force of countermeasures.<sup>[145]</sup> According to the ILC, “questions concerning the use of force in international relations . . . are governed by the relevant primacy rules” and not by the law of state responsibility. Following this reasoning, the *Articles of State Responsibility* provided no guidance on the specific question of whether forcible countermeasures that triggered article 2(4) would be *per se* illegal, leaving it for analysis under the Charter. On the one hand, some commentators have argued that based on the dicta in *Nicaragua*, the ICJ seems to have “implicitly left open the door for proportionate forcible

countermeasures” in the case of a victim state suffering from hostile acts that are not at the threshold of an armed attack.<sup>[146]</sup> On the other hand, commentators have argued that the obligation to refrain from the use of force under the Charter has been recognized as a limitation to countermeasures.<sup>[147]</sup> The *Tallinn Manual* experts were unable to reach agreement on this point and therefore offered no rule prohibiting the use of force countermeasures that would violate article 2(4).<sup>[148]</sup> Interestingly, one of the ICJ judges recently provided an interpretation of the Court’s opinion with respect to countermeasures, one that is in contrast with previously offered interpretations. At a celebration of the ICJ’s anniversary, Judge Yusuf stated, in referring to the *Nicaragua* case, “[T]he Court did not specify the nature of such ‘countermeasures,’ but it could perhaps be reasonably assumed that it was referring to military countermeasures.”<sup>[149]</sup> One reasonable understanding based on the Judge’s interpretation of the Court’s opinion would be that lawful countermeasures may include the armed force that would violate article 2(4). Another understanding of this interpretation is that countermeasures could include armed force that was never meant to be covered by article 2(4).

Perhaps a more effective way to address this debate would be to adopt a more limited meaning of what a use of force is under article 2(4). In using this approach, as discussed earlier, one could argue that there are uses of armed force that do not enter the scope of the Charter’s article 2(4) because of the low intensity of the force involved, and the context of the use of force. Rather than article 2(4) as the relevant law for those actions not covered, the focus would be on other legal regimes that may be relevant to the context of the situation. Using this standard of a more limited view of the meaning of use of force in article 2(4) would alleviate the tension over whether countermeasures can be forcible since by allowing for minimal force that is not prohibited by article 2(4), countermeasures could involve force of a minimal level that would not violate article 2(4) and therefore would be lawful under the law of countermeasures.<sup>[150]</sup> This would also allow states that are victims of uses of force that violate article 2(4) but that do not rise to the level of an armed attack to take forcible action, albeit limited in scope and intensity, in another state’s territory as long as it is proportionate to the injury and intended only to get the state to comply with its obligations. Rather than limiting the victim state to non-forcible responses that may not be effective in getting the wrongful state to comply with its legal obligations, under a more limited meaning for article 2(4) uses of force, a state may use forcible proportionate countermeasures, including cyber countermeasures. Such cyber responses would be allowed whether or not the initial wrong exhibited through cyber operations or otherwise.<sup>[151]</sup> While these actions may violate the sovereignty of the state or other bodies of law, they would not be violations of article 2(4).

In choosing what countermeasures to employ, the state has considerable flexibility in choosing which obligations to violate vis-à-vis the other state, without publicly disclosing

the basis for its attribution assessment of the prior wrongful acts of the targeted state to the targeted state. The state conducting the countermeasure ought to take care that its attribution is accurate to avoid any political consequences. If, however, the acting state in taking countermeasures was mistaken as to fact or law, and, for instance, employs countermeasures against a state that has not conducted any wrongful act, such countermeasures may still be considered lawful. Although this issue of responsibility for a mistake is a debatable point in international law, some have argued that since there is no general principle under international law as to a “fault standard in the commission of a wrong” nor is international law a system of strict liability, such countermeasures taken in error, if based on good faith, will be excused.<sup>[152]</sup> The claims and counterclaims of states after incidents of uses of military force made in error that were not considered wrongful, often settled with an apology, as well as the decisions of tribunals in relation to countermeasures, have suggested that states may be excused for countermeasures taken in error but based on good faith.<sup>[153]</sup> The opposing view, accepted by the ILC and the *Tallinn Manual* is that those states taking countermeasures “do so at their own risk” and will incur responsibility if in relying on erroneous facts or legal interpretations the state conducts an illegal countermeasure.<sup>[154]</sup>

In accordance with judicial precedence and the *Articles of State Responsibility*, there are a number of substantive and procedural requirements for countermeasures.<sup>[155]</sup> One such substantive requirement is that the countermeasure’s sole purpose must be to get the offending state to comply with its international obligations, discontinue its wrongful acts and/or provide reparation; therefore, the use of countermeasures to punish or retaliate is prohibited, can only be taken once a wrongful act has taken place, not in an anticipatory manner, and must end when the state has complied with its obligations, which could include making reparations.<sup>[156]</sup> In seeking compliance by the wrongfully acting state, the state carrying out the countermeasures, when feasible, should give notice of its intent to use countermeasures,<sup>[157]</sup> hereby providing the state an opportunity to comply. This preference for notice, however, has been interpreted as not mandatory and will depend on the particular circumstances.<sup>[158]</sup> If, for instance, giving notice would result in a less effective countermeasure then notice would not be required.<sup>[159]</sup> In addition, because the purpose of countermeasures cannot be punitive, the measures taken should be reversible, if possible.<sup>[160]</sup>

While countermeasures must be targeted only at the state responsible for the wrongful act,<sup>[161]</sup> this requirement does not prohibit countermeasures against private entities within that state in order to get the state to change its behavior and comply with its legal obligations.<sup>[162]</sup> Importantly, especially in the context of cyber countermeasures where actions may inadvertently impact third states, such effects, as long as there is no breach of a legal obligation owed to the third state, would not result in the countermeasures being unlawful.<sup>[163]</sup>

Commonly cited examples of non-forcible countermeasures that states have employed include the seizure of assets of foreigners, trade embargoes, and breaches of treaties such as bilateral aviation agreements. Examples of non-forcible *cyber* countermeasures could include “blocking electronic access to a state’s bank accounts” contrary to an applicable treaty provision.<sup>[164]</sup> Measures that have been characterized as countermeasures with minimal force, not covered by article 2(4) under a *de minimis* or gravity threshold approach, include shooting across a ship’s bow in response to violations of fishing quotas, forced landing or shooting of an aircraft within a state’s airspace without authorization, abduction of criminals in another state’s territory without consent, and the rescue of nationals abroad.<sup>[165]</sup> As long as it has been determined that these actions would be proportionate to the injury that was suffered, taking into consideration the principles at stake from the wrongful act, such countermeasures carried out by cyber means would be lawful since they do not constitute a violation of article 2(4).

Under the *de minimis* standard for article 2(4), an example of a lawful forcible *cyber* countermeasure involving minimum force could involve the disabling of Internet access routers of a state within that state’s territory, denying the state access to the Internet. While this action may constitute a violation of the state’s territorial sovereignty by the action taken in the territory of that state, it would not be covered by article 2(4) because of the *de minimis* nature of the force. In contrast, a *cyber* countermeasure that included the bricking or destruction of all routers in another state, causing irreversible damage to critical infrastructure, would likely be covered by article 2(4) and, reaching the requisite level of force, would not be permissible under the law of countermeasures.

In circumstances where a state’s reply to hostile *cyber* operations cannot be justified as a lawful countermeasure, for instance, if such measures would fail to meet any of the requirements for countermeasures, the state could still act to prevent imminent or ongoing hostile *cyber* operations that represent a “grave and imminent peril” to the “essential interests” of the state pursuant to a “plea of necessity.”<sup>[166]</sup> Although the plea of necessity was once considered “marginal,” there is substantial authority for its existence from state practice and international tribunals that have either accepted the principle as a circumstance precluding wrongfulness or at least not rejected it as such.<sup>[167]</sup> Similar to countermeasures, this concept of necessity, although not anchored in any conventional provision of law but being in principle accepted by a growing number of states, permits a state to escape liability under the law of state responsibility for its actions that would normally constitute a violation of international law, whether a treaty or customary obligation.<sup>[168]</sup>

While there is a recognized trend that this defense of necessity is “now coming to the forefront of public international law, suggesting that more and more states will argue necessity in the future. . .,”<sup>[169]</sup> necessity is controversial and has only been accepted as an exceptional rule. In the 19th and 20th centuries, concerns raised about states abusing

necessity by using it as a pretext to justify armed attacks against other states, resulted in the development of stringent requirements for the plea designed to carefully constrain the doctrine to a narrowly defined set of circumstances.<sup>[169]</sup> Today, it remains unsettled as to whether necessity can be invoked to justify forcible actions that would violate article 2(4) of the Charter, both in the context of traditional military kinetic operations as well as cyber operations.<sup>[170]</sup> However, for actions under a plea of necessity, just as with countermeasures, that are forcible but not covered by article 2(4) because of their limited intentions and purposes which bear no relation to the purposes characteristic of true uses of force as meant by article 2(4), such actions under necessity could be justified.

As distinguishable from the conditions required for countermeasures, the conditions for the application of necessity can be divided into two categories. The first category relates to balancing conflicting interests at stake and includes four constitutive elements: a) an essential interest of the state invoking the necessity is at stake, b) an interest is threatened by a grave and imminent peril, c) the action must be the only means to guard against the peril, and d) the interest to be disregarded in taking the action must be of lesser value than the interest being safeguarded. The second category includes circumstances of an absolute preclusion to invoking the defense: when the primary rule at issue, such as the use of force regime of the Charter, excludes the possibility of invoking the principle and when the state whose interest is threatened substantially contributed to the occurrence of the situation of necessity.<sup>[171]</sup>

Although there is no accepted definition of what would constitute “essential interests” of a state under international law, examples from international cases and state practice have included issues related to a state’s security, the preservation of the state’s natural environment or the ecological equilibrium, economy, public health, safety, and maintenance of the food supply for the population.<sup>[172]</sup> As to the element of grave and imminent peril, what is required is that the “peril is clearly established on the basis of the evidence reasonably available at the time”<sup>[173]</sup> and the prohibited actions taken are to be “the only way for the State to safeguard” its essential interests, leaving no other legitimate choices left for the state.<sup>[174]</sup> The actions must also not affect the vital interest of any other state in a grave and imminent way.<sup>[175]</sup> In other words, the interest sought to be protected by the state in conducting the actions under the plea must be of greater importance than the other state’s interest that will be temporarily disregarded.

In contrast to countermeasures and self-defense, actions based on necessity do not require any initial wrongful act, and therefore attribution is not necessary.<sup>[176]</sup> In the cyber context, given that attribution challenges persist, this may make necessity particularly useful in the face of grave threats through cyberspace. Furthermore, unlike countermeasures, which cannot be invoked in anticipation of a legal obligation being breached, actions

under necessity can take place before the culmination of the grave threat to the state's interests, anticipating the grave harm that will ultimately emerge.<sup>[177]</sup> As a cautionary note, actions under necessity have been found by courts to be permissible only under what is considered exceptional circumstances when the situation constitutes a grave and imminent peril to the essential interests of the acting state.<sup>[178]</sup>

Although the standard for invoking necessity is high and circumstances allowing it are exceptional, the nature of state cyber operations, in particular, those targeting critical infrastructure, may be the circumstances that meet the high standards for necessity. In cyberspace where threats can materialize almost instantaneously through the Internet, bringing to a halt the functions of critical infrastructure that support essential state functions, target states may not have the time to seek cooperative measures from other states from which the threats emanate, or transit through, or obtain provisional measures from a Court, to eliminate the threat. Furthermore, the states whose territory is impacted by the impending peril may lack the means to take effective measures to stop the situation. As an example, consider the case of highly disruptive cyber operations against a state's banking system that would result in the loss of critical financial services and commerce to a state's population. In this situation, to prevent the harm, the state may need to respond immediately, without first attributing the attacks, and block access to some of its infrastructure from specific countries which it has existing treaty obligations with that guarantee access to the relevant infrastructure. In such a case, a justified action based on necessity could include blocking access within the responding state or if necessary in the territory of the other state from which the operation is emanating.

In a different context where a state discovers malware on a gas pipeline control system in its territory, malware that is preprogrammed to be activated in the future that will result in the disruption of the system, preventing the pressure relief function from properly working and potentially leading to a rupture of the pipeline that would jeopardize the safety of the pipeline workers and the surrounding civilian population, actions under a plea of necessity would likely be justified. In this case, it may be that in conducting its cybersecurity operations, the pipeline company finds and removes all of the malware that can be removed while keeping the system operational but locates other malware that cannot be removed without shutting down systems that are critical to the safe operation of the pipeline. In this case, the state could invoke the plea of necessity and take actions to eliminate the threat or allow the company to take such actions. It may be necessary to take action beyond the state's borders as the only means of preventing the malware from triggering and disrupting the pipeline operations. In the case where the blocking of IP addresses would not be sufficient to prevent the impending harm, and there is no time or means for the state from whose territory the command and control servers reside to take the necessary measures, or the state is unwilling to take the necessary steps, a cyber response under a plea of necessity could entail hacking back and shutting down cyber infrastructure

in that territory that is being used to mount the harmful operations as long as by doing so would not seriously impair the essential interests of any affected state.<sup>[179]</sup> In the face of the grave and imminent, and otherwise, unavoidable danger to the essential interests of the state from the pipeline failure, the state would be justified in violating its international obligations owed to the other state.

In cases of cyber operations targeting critical infrastructure that would result in “severe negative impact” on the target state’s “security, economy, public health, safety, or the environment,” the necessity plea is available to states as a last resort and may be particularly relevant given the nature of cyberspace and hostile cyber operations and the international rules related to the use of force and state responsibility.<sup>[180]</sup> In circumstances similar to the pipeline example where logic bombs are found on networks and attribution for the implants is not possible or time does not allow for it, countermeasures will be unavailable. Furthermore, given that current uncertainty about if and how the general principle of sovereignty applies to cyber activities, in particular to unconsented territorial interference in computer networks of another state,<sup>[181]</sup> the issue of the legality of implanting malware in another state’s infrastructure is left unclear, thereby leaving countermeasures unavailable without a clear prior wrongful act in the case of implanted malware. Under these circumstances, the plea of necessity may present the only lawful option for the state in preventing the harm to its essential interests.

## CONCLUSION

Traditionally, international law maintained a strict division between war and peace, holding *inter bellum et pacem nihil est medium* – there was no intermediate state between war and peace.<sup>[182]</sup> Of course, in those times it was seldom difficult to determine whether armed force was being employed, triggering a state of war, and which state’s forces were involved. Describing a very different security environment today, the 2017 *U.S. National Security Strategy* (NSS) warns that the factual dividing line between peace and war has become more difficult to determine, describing current international relations as more of “an arena of continuous competition.”<sup>[183]</sup> As the former British Secretary of State for Defense recently declared, contemporary adversaries are deliberately seeking to “blur the lines between what is, and what is not, considered an act of war.”<sup>[184]</sup>

Although determinations of the facts on the ground may be more challenging in the context of cyber operations, where technological developments and networked communications have allowed states to more easily use proxies to disguise their actions, enabling their hostile actions to remain below a level that would provoke a full-scale response, the Grotian divide between war and peace still remains a vital part of the international legal order in support of international stability. Key to the Grotian notion, however, is clarity about the legal thresholds that divide peace from war as well as the redlines for

the legality of actions during both times of peace and times of war. But as the NSS points out, adversaries are exploiting existing international law principles that are ambiguous or subject to competing interpretations in all domains as they operate on the edge between peace and war. In doing so, they hope to avoid any serious consequences for violating the laws that have developed through treaties and custom. Efforts to counter these threats will require addressing these legal ambiguities that are currently inhibiting state responses and allowing violators to escape repercussions.

As international law is sure to evolve as it has done historically in the face of new threats and technologies, it will be for states to drive this evolution. Whether they will eventually consent to rules within a treaty for cyber operations or not remains to be seen. The law, however, will also evolve through the consent of states in their practices out of a sense of legal obligation, *opinio juris*, which can eventually crystallize into customary international law. Coupled with the decades of state practice of employing cyber operations in their strategic and military activities, the recent public statements by government officials concerning the interpretation of international law as applied to those cyber operations serve to develop and reaffirm interpretations of international rules, tailoring them for this domain.<sup>[185]</sup> These trends will help address the gray zone conflicts, including the cyber operations that are part of those conflicts, and diminish the advantages adversaries are seeking to gain in this space. In doing so, states will shrink the area of gray zone conflicts, providing fewer opportunities for states to exploit gray zones, and generate much-needed stability in cyberspace, support for the development of effective frameworks for national policy, doctrine and rules of engagement for cyber operations, and enhanced deterrence within the global cyber domain.<sup>[186]</sup> 

## NOTES

1. Ellen Nakashima, "When Is a Cyberattack an Act of War?" *The Washington Post*, October 26, 2012, [https://www.washingtonpost.com/opinions/when-is-a-cyberattack-an-act-of-war/2012/10/26/02226232-1eb8-11e2-9746-908f727990d8\\_story.html?utm\\_term=.79f2f366be90](https://www.washingtonpost.com/opinions/when-is-a-cyberattack-an-act-of-war/2012/10/26/02226232-1eb8-11e2-9746-908f727990d8_story.html?utm_term=.79f2f366be90).
2. Morgan Chalfant, "Democrats Step Up Calls that Russian Hack Was an Act of War," *The Hill*, March 26, 2017, <http://thehill.com/policy/cybersecurity/325606-democrats-step-up-calls-that-russian-hack-was-act-of-war>.
3. Mark Pomerleau, "Intelligence officials: Cyber domain is still the 'Wild West'," *Cyber Defense*, 2015 (quoting testimony from Deputy Secretary of Defense Robert Work before the Senate Armed Services Committee stating, "[T]here's no defined red line for what would constitute an act of war."), <http://defensesystems.com/articles/2015/09/30/in-congress-cyber-wild-west.aspx>. Mike Rounds, "Defining a Cyber Act of War: The Rules Regarding This Dangerous Threat Aren't Clear – Some Concision Is Urgently Needed," *Wall Street Journal*, May 8, 2016, <http://www.wsj.com/articles/defining-a-cyber-act-of-war-1462738124>.
4. Clyde Eagleton, "An Attempt to Define War," 291 *International Conciliation* (1933), 237, 281.
5. Yoran Dinstein, *War, Aggression and Self-Defence* (3d ed. 2001), 13 ("War is a hostile interaction between two or more States . . . in the technical sense is a formal status produced by a declaration of war . . . in the material sense is generated by actual use of armed force, which must be comprehensive on the part of at least one party to the conflict.") [hereinafter Dinstein, *War, Aggression and Self-Defence*].
6. U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, January 2018, <https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
7. Speech by Valery Gerasimov, chief of the general staff of the Armed Forces of the Russian Federation, February 2013 ("In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template."). Gerasimov's speech was translated by Robert Coalson and reprinted in his "Top Russian General Lays Bare Putin's Plan for Ukraine," *Huffington Post*, September 2, 2014; accessed February 19, 2018 at [https://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine\\_b\\_5748480.html](https://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html).
8. U.S. Special Operations Command, *White Paper: Defining Gray Zones Challenges* 1, April 2015, <https://army.com/sites/army.com/files/Gray%20Zones%20-%20USSOCOM%20White%20Paper%209%20Sep%202015.pdf>. ("[G]ray zone challenges are defined as competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality."). See also, Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, 1-2 (Carlisle, PA: United States Army War College Press, 2015) (defining gray zone conflicts where adversaries "employing gradual steps" remaining "below thresholds that would generate a powerful U.S. or international response, but nonetheless are forceful and deliberate, calculated to gain measurable traction over time . . . in the ambiguous no-man's land between peace and war . . .").
9. See Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," 42 *Yale J. Int'l. Law* 1, 2 ("The DNC hacks epitomized the grey zone strategy."). [hereinafter Schmitt, *Grey Zone*].
10. Statute of the International Court of Justice, Annexed to the Charter of the United Nations, 1945, 9 Int. Leg. 510, 522 [hereinafter ICJ Statute]. Treaties and customary international law are two of the main sources of international law. Unlike treaties that are negotiated and written by states, custom is generally non-written and comes into being when there is "evidence of practice accepted as law." ICJ Statute, art. 38.
11. For agreements by states as to the international norms and legal rules that apply to cyber operations see Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 24, UN Doc. A/70/174 (July 22, 2015) [hereinafter *UNGGE 2015 Report*]. The US has consistently stated its position that international law applies to state activities in cyberspace. See, U.S. Government, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, 8-10. U.S. Department of Defense, Office of General Counsel, *Department of Defense Law of War Manual*, updated December 2016, (2015), 16.3.2 ("International law and long-standing international norms are applicable to State behavior in cyberspace.") [hereinafter *DoD Law of War Manual*]. See also, Brian J. Egan, Legal Advisor, Department of State, Remarks Delivered at Berkeley Law School, "Remarks on International Law and Stability in Cyberspace," November 10, 2016, <https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf> [hereinafter *Egan Speech*].

## NOTES

12. Thomas M. Franck, *Fairness in International Law and Institutions*, 260 (1995). Similar to treaties, customary law is a primary component of international law. Under the standard view, customary international law is conceived of as having two components: an objective, state practice element, and a subjective, sense of legal obligation component, or *opinio juris*. International tribunals as well as state have endorsed this account of customary international law. See, e.g., *Jurisdictional Immunities of the State* (Germany v. Italy), (Feb. 3, 2012), ICJ 99, 122; *North Sea Continental Shelf Cases* (Fed. Rep. Ger. V. Denmark), (Feb. 20, 1969) ICJ 4, 44; Special Rapporteur, *Second Report on Identification of Customary International Law*, 9-10, Int'l L. Comm'n, UN Doc. A/CN.4/672, May 22, 2014.
13. Michael N. Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical *Vade Mecum*," 8 *Harvard National Security Law Journal* (2017), 239, 242. ("While there is no longer any serious debate as to whether international law applies to transborder cyber operations, the international community has been unable to achieve consensus on the precise application of many international law principles and rules that govern them.") [hereinafter Schmitt, *Peacetime Cyber Responses*].
14. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 19, UN Doc A/68/98, (June 24, 2013), 8, [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/68/98](http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98). ("[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.")
15. See *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* (Michael N. Schmitt ed., 2013) (Cambridge: Cambridge University Press, 2nd ed. 2017) [hereinafter *Tallinn Manual 2.0*]. See also, Yoram Dinstein, "Computer Network Attacks and Self-Defense," *International Law Studies* 76 (2002), 103 [hereinafter Dinstein, "Computer Network Attacks"]. Marco Roscini. *Cyber Operations and the Use of Force in International Law* (2014) [hereinafter, Roscini, *Cyber Operations*].
16. See Arun Mohan Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?," *Lawfare*, July 4, 2017, <https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>. Michele G. Markoff, Deputy Coordinator for Cyber Issues, US Department of State, "Remarks as Prepared for The Chairman, UN GGE: Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security," June 23, 2017, <https://usun.state.gov/remarks/7880>. See also, Catherine Lotrionte, "Geopolitics Eclipses International Law at the UN," *Cipher Brief*, August 6, 2017.
17. *Tallinn Manual 2.0*. The *Tallinn Manual* is a compendium of rules and commentary that were developed by international legal experts in assessing the applicability of international law to cyber operations. Although the rules do not reflect settled international law, and no state has accepted the rules generally as reflective of the law, the rules and commentary have garnered much international attention, and concern, justifying a close review of them. For an overview of the purpose of the Tallinn Manual project as well as analysis of some of its rules see Schmitt, *Peacetime Cyber Responses*.
18. The Hague Convention IV Respecting the Laws and Customs of War on Land, 18 October 1907, 36 Stat. 2277; The Hague Regulations, Convention IV Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 18 October 1907, 36 Stat. 2277. See also Ian Brownlie, *International Law and the Use of Force by States*, (1963), 80-83.
19. Covenant of the League of Nations, 225 Parry 195; 1 Hudson I; 112 BFSP 13; 13 AJIL Supp. (1919), 128.
20. General Treaty for Renunciation of War as an Instrument of National Policy, August 27, 1928, 46 Stat. 2343, 94 LNTS 57 [hereinafter the *Kellogg-Briand Pact*].
21. See Lassa Oppenheim, *International Law* 225, 93 (Sir Hersch Lauterpacht ed., 7th ed. 1952).
22. See Mary Ellen O'Connell, ed., *What is War?: An Investigation in the Wake of 9/11*, Martinus Nijhoff/Brill Publishers, 9-10.
23. Jean Pictet, 9ed., *Commentary on the Geneva Conventions of August 12, 1949*, Vol. 1: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (ICRC, Geneva 1952) 32 ("Any difference arising between two States and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2 [of the Geneva Convention], even if one of the Parties denies the existence of a state of war."); Marco Sassòli, Antoine Bouvier and Anne Quintin, *How Does Law Protect in War?* (Vol.1, 3rd edition, ICRC, Geneva 2011) 34 ("[A]s soon as the first (protected) person is affected by the conflict, the first segment of territory occupied, the first attack launched" then international humanitarian law starts to apply).

## NOTES

24. See *Tallinn Manual 2.0*, Rule 82 and 83, at 290, for a discussion of the applicability of international humanitarian law to international and non-international armed conflicts in the cyber context. See also Michael N. Schmitt, “The Law of Cyber Warfare: *Quo Vadis*,” 25 *Stanford Law & Policy Review*, 289-299 (2014) [hereinafter Schmitt, “Law of Cyber Warfare”].
25. *UN GGE 2015 Report*.
26. Kellogg-Briand Pact, art. 1; UN Charter, art. 2(4).
27. *Military and Paramilitary Activities* (Nicar. v. US), 1986 ICJ (June 27), 14, 99-100, [hereinafter *Nicaragua*].
28. See also, Yoram Dinstein, *War, Aggression and Self-Defence*, 94. *International Law Commission Yearbook*, 1966, 1966-II, 247, para. 1. In international law, *jus cogens* norms are those legal rules from which no derogation is permitted. See International Law Commission, *First Report on Jus Cogens*, Sixty-Eighth Session, UN Doc. A/CN.4/693, March 8, 2016 (prepared by Special Rapporteur, Mr. Dire Tladi).
29. UN Charter, Preamble, U.N.T.S., Vol. 16, 1 ff.
30. 6 Documents of the United Nations Conference on International Organization (1945), 339, 334–35; Conference on Int’l Org., S.F., Cal., April 25, 1945, Commission I: General Provisions, art. 7, para. 4.
31. UN Charter, art. 2(4).
32. See Albrecht Randelzhofer, “Article 2(4),” *The Charter of the United Nations: A Commentary* 106, 112-113 (Bruno Simma ed., 1995) [hereinafter, Simma, *Charter of the United Nations*]. See also Yoram Dinstein, *War, Aggression and Self-Defence* 88 (5th ed. 2011) (“the term ‘force’ in Article 2(4) must denote violence. It does not matter what specific means—kinetic or electronic—are used to bring it about, but the end result must be that violence occurs or is threatened.”).
33. Mary Ellen O’Connell, “The Prohibition on the Use of Force,” in *Research Handbook on International Conflict and Security Law* 89, 101 (Nigel D. White & Christian Henderson eds. 2013) [hereinafter O’Connell, *Use of Force*]. (“Excluded from the scope of Article 2(4) are such coercive measures as economic sanctions; diplomatic protest; physical force not involving weapons, such as cutting the nets of fishing vessels; disrupting internet service by denial of service attacks; and unconsented presence of official vessels or vehicles within another state’s jurisdiction.”). See also, *Corfu Channel Case* (UK v. Albania) (Judgment) (1949) ICJ Rep. 4, 35 [hereinafter *Corfu Channel*].
34. See Olivier Corten, *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law* (Oxford and Portland: Hart, 2010) (“[W]hat matters, besides an abstract evaluation of the gravity of events [in assessing what is a use of force] is to determine whether there is an intention on the part of a State to use force against another State.”), 201 [hereinafter Corten, *Law Against War*]. Corten’s work is the most comprehensive account of state practice relating to the scope of “use of force” for the Charter purposes. See *Case Concerning Oil Platforms* (Iran v. US), Merits, Judgment, November 6, 2003, ICJ Reports 2003, para. 52, 61, 64 [hereinafter *Oil Platforms*]; *Nicaragua*, para. 231 (“Very little information is . . . available to the Court as to the circumstances of these incursions or their possible motivations, which renders it difficult to decide whether they may be treated . . . as amounting, singly or collectively, to an “armed attack” . . .”). See also, Harold Koh, “International Law in Cyberspace,” Speech at the USCYBERCOM Inter-Agency Legal Conference, September 18, 2012, in CarrieLyn D. Guymon (ed.), *Digest of United States Practice in International Law*, 2012, 598, <http://www.state.gov/documents/organization/211955.pdf>, [hereinafter *Koh Speech*] (“In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and *intent*, among other possible issues.”) (emphasis added).
35. O’Connell, *Use of Force*, 102 (“Article 2(4) is narrower than it might appear on its face. Minimal or de minimis uses of force are likely to fall below the threshold of the Article 2(4) prohibition.”). See also, Corten, *Law Against War*, 55.
36. Corten, *Law Against War*, 52-78.
37. See Colonel Gary P. Corn, “Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace,” in *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, 62-64 (Oxford University Press, forthcoming), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3089071](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3089071), (arguing for sovereignty as a foundational principle only)[hereinafter Corn, “Cyber National Security”]. For the contrary position arguing that sovereignty is a primary rule of international law, see Michael N. Schmitt & Liis Vihul, “Respect for Sovereignty in Cyberspace,” 95 *Texas Law Review* 1639 (2017) [hereinafter, Schmitt & Vihul, “Respect for Sovereignty”]. For this position see also *Tallinn Manual 2.0*, 168-174.

## NOTES

38. Speech by Attorney General Jeremy Wright QC, UK, “Cyber and International Law in the 21st Century,” May 23, 2018, <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>, [hereinafter *UK AG Speech*]; *Koh Speech*; *Egan Speech*.
39. Tom Ruys, “The Meaning of “Force” and the Boundaries of the Jus Ad Bellum: Are “Minimal” Uses of Force Excluded From UN Charter Article 2(4)?” 108 *Am. J. Int’l L.* 159 (2014), (the author “concludes that excluding small-scale or “targeted” forcible acts from the scope of Article 2(4) is conceptually confused, inconsistent with customary practice, and undesirable as a matter of policy.”) [hereinafter Ruys, *Meaning of Force*].
40. Corten, *Law Against War*, 52-78; See also *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, (1996) ICJ 14, 246-247, para. 48, (In assessing whether there was a violation of article 2(4), “depends upon whether the particular use of force envisaged would be directed against the territorial integrity or political independence of a State, or against the Purposes of the United Nations or whether, in the event that it were intended as a means of defence, it would necessarily violate the principles of necessity and proportionality.”). [hereinafter *Nuclear Weapons*]. See also, A Randelzhofer, “Article 2(4)” in Simma, *The Charter of the United Nations*, 123 (“As the prohibition of the threat or use of force is limited to the international relations between States it is the opinion of various authors that this prohibition does not comprise military acts of protection within the State territory against intruding persons or aircraft.”).
41. *Corfu Channel*, 35 (“Between independent States, respect for territorial sovereignty is an essential foundation of international relations . . . [T]he Court must declare that the action of the British Navy constituted a violation of Albanian sovereignty.”).
42. *Id.*, 34-35.
43. See Corten, *Law Against War*, 55-67.
44. *Id.*, 52-66.
45. Schmitt, *Peacetime Cyber Responses*, 245 (The *Tallinn Manual 2.0* experts were unable to agree on “when cyber operations not having those consequences [of damage or injury] qualify” as a use of force.). Michael N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,” *Columbia Journal of Transnational Law* 37 (1998-99), 914-915 [hereinafter Schmitt, “Computer Network Attack”]. The author proposes a list of eight, non-exhaustive factors that states may consider in order to establish when the scale and effects of cyber operations that produce negative effects but non-physical in nature that may resemble that of kinetic uses of force to include, severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality. These factors, as the author admits, are “not legal.” See Michael N. Schmitt, “The Use of Force’ in Cyberspace: A Reply to Dr. Ziolkowski,” in *2012 4th International Conference on Cyber Conflict* (2012), edited by Christian Czosseck, Rain Ottis and Katharina Ziolkowski, 314. *Tallinn Manual 2.0*, 234-236, 337 (adopting the above factors and the following additional factors for consideration in assessing whether an action constitutes a use of force: “the prevailing political environment, whether the cyber operation portends the future use of military force, the identity of the examiner, and record of cyber operations by the attacker, and the nature of the target.”). *Koh Speech*.
46. See *Tallinn Manual 2.0*, 333 (Describing cyber uses of force as “[A]cts that injure or kill persons or physically damage or destroy objects are uses of force.”). See also, Schmitt, *Peacetime Cyber Responses* (noting that non-state actors cannot conduct a use of force as meant by article 2(4) of the Charter.)
47. *DoD Law of War Manual*, 998-999 (“Cyber operations that constitute uses of force within the meaning of Article 2(4) of the Charter of the United Nations and customary international law must have a proper legal basis in order not to violate *jus ad bellum* prohibition on the resort to force.”).
48. Dinstein, “Computer Network Attacks,” 103. See Eric Talbot Jensen, “Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,” 38 *Stanford Journal of International Law* (2002), 207, 209.
49. Roscini, *Cyber Operations*, 46-47. The effects-based approach has been embraced by the United States for cyber operations. *Koh Speech*, 598 (“if the physical consequences of a cyber-attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber-attack should equally be considered a use of force.”). See also, *Tallinn Manual 2.0*, Rule 69, 330 (“[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.”). See Schmitt, “The Law of Cyber Warfare,” 269, 281 (“a cyber operation as a use of force . . . causing greater than *de minimis* damage or injury suffices.”).

## NOTES

50. See *DoD Law of War Manual*, 998-1000 (listing examples of cyber operations that would cross the threshold of a use of force – triggering a nuclear plant meltdown, opening a dam above a populated area and causing destruction; disabling air traffic control services, resulting in airplane crashes and the crippling of a military’s logistics systems.).
51. See, e.g., Marco Roscini, “World Wide Warfare – The Jus ad Bellum and the Use of Cyber Force,” 14 *Max Planck Yearbook United Nations L.*, (2010), 85.
52. Gary Brown and Keira Poellet, “The Customary International Law of Cyberspace,” *Strategic Studies Quarterly*, Vol. 6, Issue 3 (2012), 126, 137.
53. See The President’s National Infrastructure Advisory Council, “Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure,” *Draft Report*, August 2017, <https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf>. See also, Daniel R. Coats, Director of National Intelligence, “Statement for the Record, Worldwide Threat Assessment of the Intelligence Community,” Senate Select Committee on Intelligence, May 11, 2017, <http://www.iranwatch.org/sites/default/files/os-coats-051117.pdf>.
54. Schmitt, *Peacetime Cyber Responses*, 246 (“Presumably, states will treat cyber operations with very severe consequences, such as the targeting of the state’s economic well-being or its critical infrastructure, as armed attacks to which they are entitled to respond in self-defense. This will likely be the case even when those operations are neither destructive nor injurious.”).
55. See Nils Melzer, “Cyberwarfare and International Law,” UNIDIR, 2011, 14, arguing that the kinetic equivalence doctrine used to interpret article 2(4), that considers a use of force only those cyber operations that cause material damage comparable to kinetic attacks, is too restrictive. <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>.
56. *Nicaragua*, 1986 ICJ, paras. 118-119, 228.
57. The US has argued that “under some circumstances, a disruptive activity in cyberspace could constitute an armed attack” and therefore also a use of force. UN Doc A/66/152, July 15, 2011, 18. In the context of cyber operations, legal scholars have interpreted the threshold of uses of force and armed attacks in cyber to include cyber operations against critical infrastructure with “significant effects” that may not be destructive or injurious. See, Michael Schmitt, “Armed Attacks in Cyberspace: A Reply to Admiral Stavridis,” *Lawfare*, January 8, 2015, <https://www.lawfareblog.com/armed-attacks-cyberspace-reply-admiral-stavridis>. Vida M. Antolin-Jenkins, “Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?,” 51, *Naval L. Rev.* 132 (2005), 172. Katharina Ziolkowski, “Computer Network Operations and the Law of Armed Conflict,” *Military Law and Law of War Review* 49 (2010), 74-75.
58. See Roscini, *Cyber Operations*, 62.
59. See *Nicaragua*, para. 228, see also Schmitt, “Computer Network Attack,” 885.
60. Ian Brownlie, *International Law and the Use of Force by States* 362 (5th ed. 1998). Simma, *Charter of the United Nations*, 208. Schmitt, “Computer Network Attack,” 906-908.
61. Dinstein, *War, Aggression and Self-Defence*, 81.
62. See *Nicaragua*, paras. 202, 205; *Corfu Channel*, 35. On intervention in general see Philip Kunig, “Intervention, Prohibition of,” *Max Planck Encyclopedia of Public International Law* (2012), Vol. VI, 290. For violations of the norm of non-intervention in the cyber context see *Tallinn Manual 2.0*, 312-325. For violations of the norm of sovereignty or territorial integrity in the cyber context see *Tallinn Manual 2.0*, 7-17.
63. *Nicaragua*, para. 206.
64. O’Connell, *Use of Force*, 102.
65. *Id.*
66. Ruys, *Meaning of Force*, (arguing against a minimum threshold for uses of force under article 2(4)). For arguments supporting the position of a minimum threshold for article 2(4) see O’Connell, *Use of Force*; Corten, *The Law Against War*, 77 (“there is a threshold below which the use of force in international relations, while it may be contrary to certain rules of international law, cannot violate article 2(4).”).
67. O’Connell, *Use of Force*, 102-107 (while acknowledging that “[t]here is no express authority on the point,” the author finds that “Article 2(4) is narrower than it might appear on its face.”). See also Robert Kolb, *Ius Contra Bellum* 247 (2d ed. 2009).

## NOTES

68. 2 Independent International Fact-Finding Mission on the Conflict in Georgia, *Report* 242 & n. 49 (September 2009), <http://www.ceiig.ch/Report.html>.
69. Robert Kolb, *International Law on the Maintenance of Peace: Jus Contra Bellum*, (Edward Elgar Publishing, 2018), 337. See also, O'Connell, *Use of Force*; Corten, *The Law Against War*, 55, 77.
70. James Masters, "Theresa May's full statement on Russian spy's poisoning," *CNN.org*, March 13, 2018, <https://www.cnn.com/2018/03/13/europe/theresa-may-russia-spy-speech-intl/index.html>.
71. Peter Walker and Andrew Roth, "UK, US, Germany and France unite to condemn spy attack," *The Guardian*, March 15, 2018, <https://www.theguardian.com/uk-news/2018/mar/15/salisbury-poisoning-uk-us-germany-and-france-issue-joint-statement>.
72. SC Res 138 (1960), June 23, 1960, para. 1; S/PV.865, June 22, 1960, 5, para. 26.
73. Corten, *The Law Against War*, 67.
74. Id. Corten, *The Law Against War*, Id., 55.
75. Roscini, *Cyber Operations*, 54. See *Tallinn Manual 2.0*, 334.
76. See also, I Lassa Oppenheim, *Oppenheim's International Law* 432 (Sir Robert Jennings & Sir Arthur Watts, eds., 9th ed. 1992. *Tallinn Manual 2.0*, 213-217.
77. Harold Koh statement on "intent" and "gravity" to assess whether an act is a use of force covered by article 2(4).
78. For a discussion of countermeasures under international law see pages 20-24 and accompanying endnotes.
79. In his separate judgment in *Oil Platforms*, Judge Simma supported the position for defensive actions by force in response to a "smaller-scale use of force." *Oil Platforms*, 332. For views that a right to use force may exist even when an armed attack mentioned in article 51 has neither occurred nor is imminent see Waldock, "The Regulation of the Use of Force by Individual States in International Law," 81 *Collected Courses* (1952-11), 451, 496-497. Thomas Franck, *Recourse to Force: State Action Against Threats and Armed Attacks* (2002), 12 [hereinafter Franck, *Recourse to Force*].
80. For a discussion of the requirements for countermeasures see pages 23-24 and accompanying endnotes.
81. UN Charter, art. 39, 42. See Simma, *The Charter of the United Nations*, 670-671. See Article 3(g), 1975 General Assembly Definition of Aggression, UN GA Res. 3314 (XXIX) 1974.
82. UN Charter, art. 51.
83. Derek W. Bowett, *Self-Defence in International Law* (1958), 188-189. C.H.M. Waldock, "The Regulation of the Use of Force by Individual States in International Law," 81 *Recueil des Cours* (1952 II) (1968), 451, 498 ("[w]here there is convincing evidence not merely of threats and potential danger but of an attack being actually mounted, then an armed attack may be said to have begun to occur, though it has not passed the frontier."). See Dinstein, *War, Aggression and Self-Defence*, 172-173 (discussing anticipatory self-defense as "interceptive self-defense").
84. *Koh Speech*; *UN GGE 2015 Report*; See also *Nicaragua*, paras. 176, 194; *Nuclear Weapons*, 823, paras. 41, 39 (discussing how article 51 applies to "any use of force, regardless of the weapon used"). See also *Tallinn Manual 2.0*, 339.
85. *Nicaragua*, para. 228. For anticipatory self-defense in the cyber context see Terry D. Gill and Paul A.L. Duchaine, "Anticipatory Self-Defense in the Cyber Context," *International Law Studies* 2013. Anticipatory self-defense against imminent cyber armed attacks has been incorporated in Rule 73 of the *Tallinn Manual 2.0*, 350 ("Imminence and immediacy: The right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy.").
86. See *Tallinn Manual 2.0*, 345 (the majority "concluded that State practice has established a right of self-defence in the face of cyber operations at the armed attack level by non-State actors acting without the involvement of a State, such as terrorist or rebel group."). See also Roscini, *Cyber Operations*, 85 (arguing that the right of self-defense allows states to exercise the right of self-defense against armed attacks by non-state actors, limited by necessity and proportionality).
87. *Nicaragua*, paras. 191,195 (distinguishing between armed attacks and "mere frontier incidents" based on the "scale and effects" of the former.). See Tom Ruys, *'Armed Attack' and Article 51 of the UN Charter* (Cambridge: Cambridge University Press, 2010) ("Scale" refers to the amount of armed force employed or its duration, while "effects" is the damage caused). *Tallinn Manual 2.0* incorporates the scale and effects test for assessing whether cyber operations would constitute uses of force or armed attacks. *Tallinn Manual 2.0*, 330-331, 342.

## NOTES

88. Since *Nicaragua*, the US has not recognized any difference between a use of force or an armed attack for purposes of the UN Charter and self-defense, both in kinetic operations and cyber operations. See, e.g., *DoD Law of War Manual*, para. 16.3.3.1 (citing *Koh Speech*). See also, William H. Taft IV, “Self-Defense and the Oil Platforms Decisions,” 29 *Yale Journal of International Law* (2004), 295, 299-302.

89. *Koh Speech* (“For example, cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.”). *Tallinn Manual 2.0*, para. 8 (“a cyber operation that seriously injures or kills a number of persons or that causes significant damage to or destruction of property would satisfy the scale and effects requirement.”).

90. *Oil Platforms*, 72.

91. *Tallinn Manual 2.0*, 342 (reaching no agreement on whether Stuxnet reached the threshold for an “armed attack.”). See also, Mary Ellen O’Connell, “Cyber Security without Cyber War,” *J. of Con. & Sec. L.*, 17 (2012), 201-202 (arguing that Stuxnet was a violation of the non-intervention norm); Catherine Lotrionte, “Cyber Operations: Conflict Under International Law,” *Georgetown Journal of International Affairs*, (2012), 20 (concluding that Stuxnet did not reach the threshold of an “armed attack”).

92. *Nicaragua*, para.195. See also, Eritrea-Ethiopia Claims Commission, *Jus ad Bellum (Partial Award) 2005*, para. 11, <http://www.pca-cpa.org/upload/files/FINAL%20ET%20JAB.pdf>, (“[l]ocalized border encounters between small infantry units, even those involving the loss of life, do not constitute an armed attack for purposes of the Charter.”).

93. R. Higgins, *Problems and Process: International Law and How We Use It* (1994), 250-1 (*Nicaragua* decision may undermine self-defence).

94. *Oil Platforms*, para. 72.

95. *Id.*, 57, 61 (implying that an attack on a single military platform or installation might qualify as an armed attack).

96. Dinstein, “Computer Network Attacks,” 105.

97. See *Tallinn Manual 2.0*, 342-343 (concluding that for “cyber operations that do not result in injury, death, damage, or destruction, but that otherwise have extensive negative effects” the issue “remains unsettled.”). See also, Michael Schmitt, “Cyber Responses ‘By The Numbers’ in International Law,” *EJIL: Talk!*, August 4, 2015, <http://www.ejiltalk.org/cyber-responses-by-the-numbers-in-international-law/>, (armed attacks can also “include those that seriously impair the functionality of critical infrastructure or that otherwise have devastating non-physical effects, such as crippling a State’s economic system . . .”) [hereinafter Schmitt, *By The Numbers*].

98. In 2011, the Dutch government endorsed the findings of the report issued by the Dutch Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law. In the context of the threshold for cyber-attacks to constitute an armed attack, the report stated: “A serious, organized cyber-attack on essential functions of the state could conceivably be qualified as an ‘armed attack’ within the meaning of article 51 of the UN Charter if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state. . .” Advisory Council on International Affairs, *Cyber Warfare*, No. 77, AIV/No. 22, CAVV, (December 2011), 21, [http://www.aivadvis.nl/ContentSuite/upload/aiv/doc/webversie\\_AIV77CAVV\\_22\\_ENG.pdf](http://www.aivadvis.nl/ContentSuite/upload/aiv/doc/webversie_AIV77CAVV_22_ENG.pdf).

99. Nicholas Tsagourias, “Cyber Attacks, Self-Defense and the Problem of Attribution,” *Journal of Conflict and Security Law* 17 (2012), 231 (“a cyber-attack on critical state infrastructure which paralyses or massively disrupts the apparatus of the State should be equated to an armed attack, even if it does not cause immediate human injury or material damage.”)[hereinafter Tsagourias, “Cyber Attacks”].

100. *Id.*, 232.

101. James Green, *The International Court of Justice and Self-Defense in International Law* (Oxford: Hart Publishing, 2009), 41.

102. *Nicaragua*, para.231. *Oil Platforms*, para. 64. See also, Tom Ruys, *Armed Attack*, 168.

103. *Tallinn Manual 2.0*, 342. The Group of Experts agreed with the doctrine of “accumulation” when the same state or group of states is responsible for the individual cyber operations at issue.

104. Statement by Dr. Craig Fields, Chairman, Defense Science Board, and Dr. Jim Miller, Member, Defense Science Board and Former Under Secretary of Defense (Policy) Before the Armed Services Committee, “Cyber Deterrence,” US Senate, March 2, 2017, [https://www.armed-services.senate.gov/imo/media/doc/Fields-Miller\\_03-02-17.pdf](https://www.armed-services.senate.gov/imo/media/doc/Fields-Miller_03-02-17.pdf), (“[A] **range of state and non-state actors** have the capacity for persistent cyber-attacks and costly cyber intrusions against the United States, which individually may be inconsequential [or be only one element of a broader campaign] but which cumulatively subject the Nation to a ‘death by 1,000 hacks.’”).

## NOTES

105. This article does not address the issue of the right of self-defense in cyberspace against non-state actors whose actions are not attributable to a state under international law. On that subject, see *Tallinn Manual 2.0*, 344-346.

106. See *Nuclear Weapons*, para. 41 (quoting *Nicaragua*, para. 176). The requirement of necessity entails determining that there were no other less intensive options than using force in order to stop an ongoing attack or prevent an imminent one from happening. See *Tallinn Manual 2.0*, 348-350 for discussion of the requirement of necessity for cyber operations in the context of self-defense.

107. The requirement of proportionality entails using force in self-defense to the degree it is necessary to eliminate the threat from an armed attack. Dinstein, *War, Aggression and Self-Defence*, 208-12. *Nuclear Weapons*, para. 41 (“[t]he submission of the exercise of the right of self-defence to the conditions of necessity and proportionality is a rule of customary international law” and “[t]his dual condition applies equally to Article 51 of the Charter, whatever the means of force employed.”). As to the requirements of proportionality in the cyber context, see *Tallinn Manual 2.0*, Rules 71-75, 339-356. The US affirmed in a written statement to the UN that a use of force in self-defense against a cyber-attack “must be limited to what is necessary to address an imminent or actual armed attack and must be proportionate to the threat that is faced.” UN Doc. A/66/152, July 15, 2011, 19.

108. Addendum – Eighth report on State responsibility by Mr. Roberto Ago, Special Rapporteur – the internationally wrongful act of the State, source of international responsibility (part 1), *Yearbook of the International Law Commission*, 1980, vol. II(1), A/CN.4/318/Add.5-7, para. 120 (1980) (According to Ago, “[t]he action needed to halt and repulse the attack may well have to assume dimensions disproportionate to those of the attack suffered. What matters in this respect is the result to be achieved by the “defensive” action, and not the forms, substance and strength of the action itself.”) [hereinafter Eighth report on State responsibility by Mr. Roberto Ago, Special Rapporteur].

109. O’Connell, *Power & Purpose*, 172.

110. Eighth report on State responsibility by Mr. Roberto Ago, Special Rapporteur, para. 120.

111. See *Tallinn Manual 2.0*, 339-356. *UN GGE Report 2015*.

112. See, *The United States Diplomatic and Consular Staff in Tehran (Hostages Case)*, Provisional Measures ICJ Reports, 1979, 7, where the ICJ referred to the takeover of the U.S. embassy in Tehran by student protestors as an armed attack. In contrast, see Simma, *The Charter of the United Nations*, 670-671 (Attacks on non-military targets situated outside the territory of the states are not generally regarded as coming within the definition of an armed attack.).

113. *Nuclear Weapons*, para 39 (“any use of force, regardless of the weapons employed” could constitute an armed attack for purposes of Article 51 of the UN Charter.). Karl Zemanek, “Armed Attack,” *Max Planck Encyclopedia of Public International Law* (2012), Vol. 1, 599. See also *Tallinn Manual 2.0*, Rule 71, para. 4.

114. *Oil Platforms*, para. 72.

115. Dinstein, “Computer Network Attacks,” 106-107.

116. *Tallinn Manual 2.0*, 346. In the case of a cyberattack outside the state’s territory, against the state’s non-governmental facilities, equipment or people, the Group of International Experts for *Tallinn 2.0* could not reach consensus as to the criteria that would be required in order to assess whether such a cyber operation would constitute an armed attack.

117. *Tallinn Manual 2.0*, 349. See, *DoD Law of War Manual*, para. 16.3.3.2.

118. See *UN GGE Report 2015*, para. 28(f). In the section of the report on the “application of international law” it notes that “accusations of organizing and implementing wrongful acts brought against States should be substantiated.” No further details were included regarding any agreement about what kind of, or how much, evidence would be required. In an attempt to potentially develop a new rule of international law requiring a state to publicly disclose information that was the basis of its attribution assessment of illegal cyber operations of another state, the Russians insisted this language be added to the *UN GGE 2015 Report*.

119. See Ian Brownlie, *International Law and the Use of Force by States* 21, (1963), 220.

120. B.O. Bryde, “Self-Help,” in *Encyclopedia of Public International Law*, Vol. 4, (1982), 213-15. See also R.A. Falk, “The Beirut Raid and the International Law of Retaliation,” 63 *Am. J. of Int’l L.* (1969) 429, (“at present, international society is not sufficiently organized to eliminate forcible self-help in either its sanctioning or deterrent roles.”).

## NOTES

121. Advance Policy Questions for Lieutenant General Paul Nakasone, USA Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, 27, [https://www.armed-services.senate.gov/imo/media/doc/Nakasone\\_APQs\\_03-01-18.pdf](https://www.armed-services.senate.gov/imo/media/doc/Nakasone_APQs_03-01-18.pdf).
122. See International Law Commission, Responsibility of States for Internationally Wrongful Acts, GA Res 56/83 annex, UN Doc. A/RES/56/83, December 12, 2001, art. 50(1)(a), [hereinafter *Articles of State Responsibility*]. See *Oil Platforms*, Judge Simma's separate opinion supported forcible proportionate countermeasures in response to a "smaller-scale use of force." *Oil Platforms*, para. 12, 332. For views that a right to use force may exist even when an armed attack mentioned in article 51 has neither occurred nor is imminent see Waldock, "The Regulation of the Use of Force by Individual States in International Law," 81 *Collected Courses* (1952–11) 451, 496–497. Franck, *Recourse to Force*, 12. See *Tallinn Manual 2.0*, 330.
123. *Tallinn Manual 2.0*, 79, describing how the Rules are based on the *Articles of State Responsibility*. For information on the International Law Commission's work, see <http://www.un.org/law/ilc/index.htm>.
124. *Articles of State Responsibility*, arts. 20–26 (listing six circumstances precluding the wrongfulness of conduct that would otherwise constitute a breach of an international obligation of the state concerned: consent, self-defense, countermeasures, necessity, *force majeure*, and distress.).
125. See *Articles of State Responsibility*, art. 1. See also James Crawford, *State Responsibility: The General Part* 43 (Cambridge University Press, 2013), (The *Articles of State Responsibility* "are considered by courts and commentators to be in whole or in part an accurate codification of the customary international law of state responsibility."). *Tallinn Manual 2.0*, at n. 112, 79.
126. See endnote 138 and accompanying text.
127. See Oscar Schachter, *International Law in Theory and Practice* (1995), 184–186. With the new prohibition on armed force for enforcement purposes in the UN Charter, reprisals were replaced with the term "peaceful reprisals" or coercive measures that were forcible but not in violation of article 2(4) of the UN Charter. The term countermeasures evolved to replace the term peaceful reprisal. Over time, international tribunals and the ILC determined that such actions could not be taken against the state conducting the wrongful act as a matter of punishment or revenge but only to induce that state to comply with its legal obligations. See *Articles of State Responsibility*, art. 49. See *Air Services Agreement of 27 March 1946* (US v. France), 18 RIAA 416 (1979), 54 ILR 337, 444 (in replacing the term peaceful reprisals with "countermeasures," ruled they were "contrary to international law but justified by a violation of international law allegedly committed by the State against which they are directed ...") [hereinafter *Air Services*]. See also, *Gabčíkovo - Nagymaros Project* (Hungary v. Slovakia), (1997) ICJ 7 (September 27), paras. 82, 55. [hereinafter *Gabčíkovo - Nagymaros*].
128. *Articles of State Responsibility*, chapeau to Chapter II of Part 3, para. 3. *Egan Speech* ("a State can always undertake unfriendly acts that are not inconsistent with any of its international obligations in order to influence the behavior of other States. Such acts—which are known as acts of retorsion—may include, for example, the imposition of sanctions or the declaration that a diplomat is *persona non grata*.").
129. Id. *Articles of State Responsibility*. See also James Crawford, *Fourth Report*, para. 35, UN Doc. A/ CN.4/517 and Add. 1 (2001), <http://www.un.org/documents/ga/docs/56/a5610.pdf>. *Tallinn Manual 2.0*, Rule 20, para. 4.
130. There is often some confusion on the distinction between retorsions and countermeasures. Indeed, it is often difficult to draw a distinction between a retorsion and a countermeasure when discussing "sanctions." In a general sense, countermeasures and retorsions are sanctions in that a state is seeking to exercise pressure on another state through the use of sanctions. However, sanctions are mere "unfriendly acts" (retorsions) and are always allowable when they do not imply any violation of international obligations. However, in cases where sanctions do violate an international obligation owed to a state, such sanctions would constitute countermeasures. In short, indictments and sanctions (unless unlawful) are not considered countermeasures as a legal matter. These examples would be retorsions. See, Article 30 of the *Articles of State Responsibility* Provisionally Adopted by the International Law Commission on First Reading (1996), reproduced in Report of the International Law Commission on the Work of its Forty-Eighth Session, UN Doc. A/51/10, 125.
131. Dan Roberts, "Obama Imposes New Sanctions Against North Korea in Response to Sony Hack," *The Guardian*, January 2, 2015, <http://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-theinterview>.

## NOTES

132. Office of the Director of National Intelligence, *Background to “Assessing Russian Activities and Intentions in Recent US Elections”*: *The Analytic Process and Cyber Incident Attribution*, January 6, 2017, [https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf).

133. Evan Perez and Daniella Diaz, CNN, “White House Announces Retaliation Against Russia: Sanction, ejecting diplomats,” January 2, 2017, <http://www.cnn.com/2016/12/29/politics/russia-sanctions-announced-by-whitehouse/>. See also, The White House, *Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment*, December 29, 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and>. Mark Mazzetti and Adam Goldman, “The Game Will Go On as U.S. Expels Russian Diplomats,” *The New York Times*, December 30, 2016, [https://www.nytimes.com/2016/12/30/us/politics/obama-russian-spies.html?\\_r=](https://www.nytimes.com/2016/12/30/us/politics/obama-russian-spies.html?_r=).

134. Beyond carrying out retorsions, because of the nature of the actions by North Korea and Russia were illegal under international law, the US could have also conducted countermeasures against North Korea and Russia. For an analysis of the DNC hack and possible legal responses under international law see Sean Watts, “International Law and Proposed U.S. Responses to the D.N.C. Hack,” *Just Security*, October 14, 2016, <https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/>. For legal analysis of the Sony hack see Michael N. Schmitt, “International Law and Cyber Attacks: Sony v. North Korea,” *Just Security*, December 17, 2014 (arguing that while the Sony hack most likely would not be considered a use of force or intervention under international law it was a violation of US sovereignty.), <http://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea>.

135. *Tallinn Manual 2.0*, 112. (In giving an example of a lawful retorsion, “A State may, for instance, employ an access control list to prevent communications from another State because the former enjoys sovereignty over the cyber infrastructure on its territory.”). However, the Group of Experts of *Tallinn Manual 2.0* agreed “[A] receiving State may not suspend international cyber communication services upon which a diplomatic mission or consular post relies because according to Rule 42 [of *Tallinn Manual 2.0*] it must permit the mission or post’s free electronic communications.” *Tallinn Manual 2.0*, 294. See also ITU Constitution, arts. 34(2) and 35, specifying the conditions for a state’s right to interrupt the flow of telecommunications.

136. *Articles of State Responsibility*, arts. 48, 54. See also *Tallinn Manual 2.0*, 111. Only one state, Mexico, opposed the inclusion of countermeasures in the *Articles of State Responsibility*, arguing that they “[do] not seem to accord with internationally recognized principles on the peaceful coexistence of States.” Comments and Observations received by governments, A/CN.4/488, March 25, 1998, 83.

137. See *Air Services*, para. 81 (“Under the rules of present-day international law, and unless the contrary results from special obligations arising under particular treaties . . . [a] State is entitled . . . to affirm its rights through ‘countermeasures’”). *Nicaragua*, 14, 127, para. 248. Reparations may include restitution, compensation, and satisfaction. *Articles of State Responsibility*, arts. 34-37. On reparations for cyber operations see *Tallinn Manual 2.0*, Rule 29.

138. During the drafting the *Articles of State Responsibility*, the US stated “[w]hile we welcome the recognition that countermeasures play an important role in the regime of state responsibility, we believe that the draft articles contain unsupported restrictions on their use.” *United States: Comments on the Draft Articles on State Responsibility*, 37 ILM 468 (1998). For an analysis of the US’ specific objections on the draft articles, including on countermeasures, see Sean Murphy, “U.S. Comments on ILC Draft Articles of State Responsibility,” 3 *Am. J. of Int’l L.* 95, (July 2001), 626-628 (related to countermeasures US objections included the list of restrictions in articles 50-55, the use of the word “commensurate” instead of “proportionate,” and the use of the words “rights in question” without further elaboration.) [hereinafter Murphy, “US Comments on ILC Draft Articles”]. For a list of the requirements for countermeasures in the Articles see, A list of requirements for countermeasures in the *Articles of State Responsibility* includes: a prior wrong suffered, prior notice to an offending state before commencing countermeasures, proportionality, measures shall not amount to a use of force as meant by art. 2(4) of the Charter, shall not violate human rights, shall not constitute reprisals or violate jus cogens norms, its purpose must only be to induce compliance or reparation, offer of negotiation must be occur before countermeasures are taken, and must conclude when the offending state has complied with its obligations. *Articles of State Responsibility*, arts. 22, 30-31, 33-37, 42, 48(1), 50-54. *Tallinn Manual 2.0*, Rules 20-25. See also, *Gabčíkovo – Nagymaros*. In the context of whether countermeasures can violate art. 2(4) see, *Articles of State Responsibility*, arts. 22, 52, 51, 50(1), and 52 respectively. *Tallinn Manual 2.0*, Rule 22, para. 10 (“[the experts] were divided over whether cyber countermeasures crossing the use of force threshold, but not reaching that of an armed attack, are lawful.”).

## NOTES

139. The reasons the UN GGE failed to reach agreement on a final report in 2017 included disagreements among states as to whether countermeasures were applicable to cyber operations as well as the right of self-defense. See Michael Schmitt & Liis Vihul, “International Cyber Law Politicized: The UN GGE’s Failure to Advance Cyber Norms,” *JustSecurity.org*, June 30, 2017, <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/>. See also, *UK AG Speech* (disagreeing with the Articles of State Responsibilities’ stating that a state is not “always legally obliged to give prior notification to the hostile state before taking countermeasures against it.”)

140. *Articles of State Responsibility*, art. 51 (“Countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question.”). The US had objected to the use of the word “commensurate” instead of “proportionate” since it could be misinterpreted to mean something narrower than proportionate which would not be in accord with state practice. See, Murphy, “US Comments on ILC Draft Articles,” 628. See also Lori Fisler Damrosch, “Retaliation or Arbitration – Or Both? The 1978 United States-France Aviation Dispute,” 74 *Am. J. of Int’l L.* 4, (1980), 785, 792 (In analyzing the ICJ *Air Services* decision on the proportionality of countermeasures, “it permits states to apply countermeasures that would be disproportionate in an economic sense, in order to enforce a principle.”) [hereinafter Damrosch, “Retaliation or Arbitration.”]. See *Tallinn Manual 2.0*, 127.

141. See *Yearbook of the ILC, 2001*, Vol. II (2), 135 citing to para. 7 of the commentary to art. 51 of the Article of State Responsibility (“[A] clearly disproportionate measure may well be judged not to have been necessary to induce the responsible State to comply with its obligations but to have had a punitive aim and to fall outside the purpose of countermeasures enunciated in article 49.”). See *Gabčíkovo – Nagymaros*, 55. *Air Services*, paras. 80-98. See also, *Egan Speech* (“[U]nder the law of countermeasures, measures undertaken in response to an internationally wrongful act performed in or through cyberspace that is attributable to a State must be directed only at the State responsible for the wrongful act and must meet the principles of necessity and proportionality. . .”).

142. The ICJ in *Nicaragua* cast doubt on the right of states to participate in collective countermeasures as it ruled that only the target of the unlawful intervention may legally respond. *Nicaragua*, para. 211, 110-111. See also, James Crawford, *The International Law Commission’s Articles of State Responsibility: Introduction, Text and Commentaries* (Cambridge University Press, 2002), 305 (arguing that existing state practice is scarce and mainly limited to Western states therefore the law is uncertain today) [hereinafter Crawford, *ILC’s Articles of State Responsibility*]. In contrast see, L. A. Sicilianos, “Countermeasures in Response to Grave Violations of Obligations Owed to the International Community,” in Crawford, Pellet and Olleson (eds.), *The Law of International Responsibility* (Oxford University Press, 2010), 1137 (arguing there is sufficient practice to support the view that states can take countermeasures against third states when they violate obligations owed to the international community).

143. *Articles of State Responsibility*, art. 54, paras 6-7 of the ILC’s commentary. See *Case Concerning Barcelona Traction, Light & Power Company Limited* (Spain v. Belgium) February 5, 1970, ICJ Reports 1970, para. 33, 33 (observing that obligations *erga omnes* are the “concern of all States” and “owed towards the international community as a whole”; that “all States . . . have a legal interest in their protection.”). For a detailed discussion on *erga omnes* obligations and their impact on standing and countermeasure responses in international law see Christian J. Tams, *Enforcing Obligations Erga Omnes in International Law* (Cambridge: Cambridge University Press, 2005), 231 (“at least in the case of systemic or large-scale breaches of international law . . . a settled practice [exists] of countermeasures by states not individually injured.”). *Tallinn Manual 2.0*, 132 (“[The majority of experts concluded] that States may not lawfully take countermeasures on behalf of another State. . .”).

144. In identifying the limitations for cyber countermeasures, the *Tallinn Manual 2.0* experts were unable to agree on whether such countermeasures that triggered the article 2(4) threshold of a use of force would be lawful, *Tallinn Manual 2.0*, 125. See *Articles of State Responsibility*, art. 50(1)(a), 131 (“Countermeasures shall not affect: (a) the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations”).

145. *Tallinn Manual 2.0*, Rule 22, para. 14 (“all of the Experts agreed that cyber countermeasures might not rise to the level of an armed attack”), 126. However, because the experts could not agree on whether a forcible cyber countermeasure that was not of the intensity of an armed attack would be lawful, there was “no limitation” on forcible countermeasures included in Rule 22 on countermeasures in the *Tallinn Manual 2.0*. See *Tallinn Manual 2.0*, Rule 22, paras. 10-12 (“A minority of the Experts asserted that forcible countermeasures are appropriate in response to a wrongful use of force that itself does not

## NOTES

(145. *cont.*) qualify as an armed attack . . . “), 125-126. See also, *Oil Platforms* and Judge Simma’s dissenting opinion supporting a state’s limited right to undertake proportionate countermeasures involving the use of force when confronted with “smaller-scale use of force,” not amounting to an “armed attack.” *Oil Platforms*, para. 12, 331 (separate opinion of Judge Simma). But see *Articles of State Responsibility*, art 50(1)(a), 57 (“[c]ountermeasures shall not affect . . . the obligations to refrain from the threat or use of force as embodied in the Charter of the United Nations.”).

146. Tom Ruys, *Armed Attack*, 141.

147. *Articles of State Responsibility*, Art. 50(1)(a) (“1. Countermeasures shall not affect: (a) the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations”)

148. *Tallinn Manual 2.0*, Rule 22, para. 10, 125.

149. Judge Abdulqawi A. Yusuf, Symposium: The Nicaragua Case 25 Years Later, “The Notion of ‘Armed Attack’ in the Nicaragua Judgment and Its Influence on Subsequent Case Law,” 25 *Leiden Journal of International Law* (2012), 461-470, 466.

150. Mary Ellen O’Connell, “The True Meaning of Force,” *AJIL Unbound*, August 4, 2014, <https://www.asil.org/blogs/true-meaning-force>. Judge Simma, *Oil Platforms*, dissenting opinion.

151. *Tallinn Manual 2.0*, III (“A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another State.”).

152. O’Connell, *Power & Purpose*, 248. See also Oscar Schachter, *International Law in Theory and Practice* 187 (1995); Damrosch, “Retaliation or Arbitration,” 795 (“It seems preferable to adopt a rule allowing a state to implement countermeasures without risk of later liability when it acts upon a good faith belief that it is the victim of a breach, even though that belief turns out to be erroneous . . .”). See also *Egan Speech*, 17 (“[I]nternational law generally requires [only] that States act reasonably under the circumstances when they gather information and draw conclusions based on that information.”).

153. For a review of state practice in cases of military uses of force made in error see, Corten, *Law Against War*, 79-81; Air Services, paras. 74, 77-78, 83, 90-98; Appellate Body Report, *United States – Importation Prohibition of Certain Shrimp and Shrimp Products*, WT/DSS8/AB/RW (Oct. 22, 2001) (The US was found to be using countermeasures inconsistent with GATT obligations but no responsibility was found for such measures).

154. See *Tallinn Manual 2.0*, Rule 20, para. 16 (“States taking countermeasures do so at their own risk”). *Articles of State Responsibility*, 301-310 (“A State that resorts to countermeasures based on its unilateral assessment of the situation does so at its own risk and may incur responsibility for its own wrongful conduct in the event of an incorrect assessment.”). See also, James Crawford, Special Rapporteur of the International Law Commission, *Third Report on State Responsibility*, para. 294, 79, UN Doc. A/CN.4/507/Add.3 (“Countermeasures can only be taken in response to conduct actually unlawful; and a “good faith belief” in its unlawfulness is not enough.”). The *Articles of State Responsibility* and the *Tallinn Manual 2.0* allow mistake for self-defense actions but not for countermeasures. See *Tallinn Manual 2.0*, Rule 71, para. 14 (“the lawfulness of the response would be determined by the reasonableness of the State’s assessment as to whether an armed attack was underway against it.”). It would seem that given the general reversibility of countermeasures, making the harm only temporary, the argument for mistake for countermeasures would seem even stronger more so than with acts of self-defense which can be deadly and non-reversible.

155. *Gabčíkovo –Nagymaros*, paras. 82-87 (setting down four elements of a lawful countermeasure: 1) it must be taken in response to a prior wrongful international act, 2) the injured state must call on the state conducting the wrongful act to stop or to make reparations, 3) the effects of the countermeasures must be commensurate with the injury suffered, and 4) the purpose must be to induce the other state to comply with its legal obligations.). For a discussion of the list of restrictions on countermeasures in the cyber context see Michael N. Schmitt, “‘Below the Threshold’ Cyber Operations: The Countermeasures Response Option and International Law,” 54 *Virginia Journal of International Law* 3, 697-732 (2014) [hereinafter Schmitt, *Countermeasures*]. Under Article 50(1) of the *Articles of State Responsibility*, another requirement is that certain obligations cannot be affected by countermeasures, to include obligations related to the protection of human rights (art. 50(1)(b)) and obligations related to the inviolability of diplomatic or consular agents, premises, archives and documents (art. 50(2)(b)) and other preemptory norms.

## NOTES

156. Schmitt, *Countermeasures* (“countermeasures are reactive, not prospective”). See also, *Gabčíkovo – Nagymaros*, para. 83 (Countermeasures “must be taken in response to a previous international wrongful act of another State.”), 715.
157. *Articles of State Responsibility* at art. 49(1), 52(1). *Gabčíkovo – Nagymaros*, para. 82-83. *Tallinn Manual 2.0*, 120 (“the notification requirement is not categorical . . . it may be necessary for an injured State to act immediately in order to preserve its rights and avoid further injury.”).
158. *UK AG Speech* (In describing one aspect that the UK government disagrees with the ILC about countermeasures, “we would not agree that we are always legally required to give prior notification to the hostile state before taking countermeasures against it.”).
159. *Tallinn Manual 2.0*, 120 (concluding that notice was not required if doing so would render it countermeasures ineffective.).
160. *Articles of State Responsibility*, Art. 49(1), 49(3). *Gabčíkovo – Nagymaros*, para. 87, 56-57. For reversibility considerations in the cyber context see *Tallinn Manual 2.0*, Rule 21, para. 8 (“[T]he requirement of reversibility is broad and not absolute”), 119.
161. *Articles of State Responsibility*, art 22, para. 5. See also, Schmitt, *Countermeasures*, 728-729.
162. Schmitt, *Peacetime Cyber Responses*, 258 (“countermeasures need not be in-kind nor directed at the entity that authored the internationally wrongful act”).
163. *Tallinn Manual 2.0*, 133.
164. Schmitt, *Countermeasures*, 717.
165. Corten, *The Law Against War*, 55-66.
166. *Articles of State Responsibility*, ch. V, art. 25. *Tallinn Manual 2.0*, 135.
167. See *Russian Indemnity* (Russia v. Turkey), November 11, 1912, 12 RIAA 44; *Gabčíkovo – Nagymaros*, 7; *M/V SAIGA* (No. 2), (Saint Vincent and the Grenadines v. Guinea), International Tribunal for the Law of the Sea (1999), 38 ILM 1323.
168. *Articles of State Responsibility*, art. 25 (stating that necessity may negate state responsibility if the act “(a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and (b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.”). See also *Gabčíkovo – Nagymaros*, paras. 51, 52 (“the state of necessity is a ground recognized by customary international law for precluding the wrongfulness of an act not in conformity with an international obligation.”). *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004 I.C.J., 136, ¶ 140 (July 9) (In applying the defense of necessity under customary law, the ICJ notes that it only applied in “strictly defined conditions.”). The arbitral tribunal constituted to hear the *Sempra Energy International v Argentine Republic* case, in its 2007 award, considered the customary international law status of article 25 of the State responsibility articles on Necessity and concluded that art. 25 reflected customary international law on the issue, stating, “This not to say that the Articles are a treaty or even themselves a part of customary law. They are simply the learned and systematic expression of the law on state of necessity developed by courts, tribunals and other sources over a long period of time.” ICSID, *Sempra Energy International v Argentine Republic*, Case No ARB/02/16, award, September 28, 2007, para 244.
169. Jens David Ohlin and Larry May, *Necessity in International Law* (Oxford University Press, 2016), 39.
170. *Yearbook of the ILC*, Report of the International Law Commission on the work of its fifty-third session, A/CN.4/SER.A/2001/Add.1 (Part 2), art. 25, at 80, para. 14 of commentary, [http://legal.un.org/ilc/publications/yearbooks/english/ilc\\_2001\\_v2\\_p2.pdf](http://legal.un.org/ilc/publications/yearbooks/english/ilc_2001_v2_p2.pdf).
171. On this point, the final version of the *Articles of State Responsibility* were silent noting that it was an issue to be dealt in accordance with a review of the relevant primary rules, such as article 2(4) of the Charter. See *Articles of State Responsibility*, Commentary to art. 25, para. 21. The Tallinn Manual experts were unable to reach a conclusion on the issue. *Tallinn Manual 2.0*, Rule 26, para. 18, 140. See Report of the ILC, 32nd Session, *ILC Yearbook 1980*, Vol. II (1), 1, 43, para. 23 (“certain actions by States in the territory of other States which, although they may sometimes be of a coercive nature, serve only limited intentions and purposes bearing no relation to the purposes characteristic of a true act of aggression.”).
172. *Articles of State Responsibility*, art. 25.

## NOTES

173. *Gabčíkovo –Nagymaros*, para. 53, 7, 41. R Ago, Addendum to the Eighth Report on State Responsibility, *ILC Yearbook 1980*, Vol. II(1), para. 78, 13, 50.
174. *Articles of State Responsibility*, Commentary to art. 25, para. 16.
175. *Articles of State Responsibility*, art. 25(1)(a). See also, Roberto Ago, “Addendum to the Eighth Report on State Responsibility” (1980, vol. II), *Yearbook of the International Law Commission* 15, 19 (In assessing how “essential” a given interest of a state must be, “it naturally depends on the totality of the conditions in which a State finds itself in a variety of specific situations: it should, therefore, be appraised in relation to the particular case in which such an interest is involved, and not predetermined in the abstract.”). Examples of “essential interests” that have been suggested include the political or economic survival of the state, the continuous functioning of essential services, the survival of a sector of the population, and the preservation of the environment. See Addendum to Eighth Report, on State Responsibility by Mr. Roberto Ago, (1980) 2 *Yearbook of International Law*, Commentary 51, para. 12, UN Doc A/CN.4/318/ADD.5-7. *Tallinn Manual, 2.0*, 135.
176. *Articles of State Responsibility*, art. 25 (1)(b). *Tallinn Manual 2.0*, 137.
177. *Tallinn Manual 2.0*, 137.
178. *Articles of State Responsibility*, Commentary to art. 25, para. 16 (“the peril is clearly established on the basis of the evidence reasonably available at the time.”).
179. Crawford, *ILC’s Articles of State Responsibility*, para. 17, 184; *Articles of State Responsibility*, Commentary to art. 25, para. 20. *Tallinn Manual 2.0*, 140.
180. Schmitt, *By The Numbers*. See also, *Tallinn Manual 2.0*, 138 (“[I]f significant cyber operations of unknown origin target its critical infrastructure, the plea of necessity could justify a State’s resort to counter-hacking.”). On the requirement of imminence, a rule of reason applies. *Tallinn Manual 2.0*, 138 (“This standard allows some degree of uncertainty as to whether the offending operation will occur, whether sufficient harm will ensue to justify a plea of necessity and the identity of the originator of the operation.”).
181. *Tallinn Manual 2.0*, 136-137 (examples of situations that gravely threaten the essential interests of a state through cyber operations that are provided include: cyber operations that would debilitate the State’s banking system, cause a dramatic loss of confidence in its stock market, ground planes nation-wide, halt all rail traffic, stop national pension and other social benefits, alter national health records, cause a major environmental disaster, among others.).
182. See Corn, “Cyber National Security” (arguing for sovereignty as a foundational principle only); Schmitt & Vihul, “Respect for Sovereignty in Cyberspace” (arguing for sovereignty as a primary rule of international law). See also, *UK AG Speech* (“Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention.”); *Egan Speech* (“[P]recisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and *opinio juris*.”).
183. Hugo Grotius, *The Law of War and Peace in Three Books* (Francis W, Kelsey tr, 1625) book III, ch. XXI, section.
184. U.S., *National Security Strategy*, December 2017, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
185. Speech by Secretary of State for Defence, UK, “Defence Secretary’s speech to RUSI on the SDSR 2015,” September 22, 2015, <https://www.gov.uk/government/speeches/defence-secretarys-speech-to-rusi-on-the-sdsr-2015>.
186. See, e.g., *UK AG Speech*.
187. For deterrence in cyberspace, see Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence Report*, February 2017; Joseph S. Nye, Jr., “Deterrence and Dissuasion in Cyberspace,” 41 *International Security* 44 (Winter 2016/17); Catherine Lotrionte, “Cyberwar: Building a Normative and Legal-Based Approach for Cyberdeterrence,” in *Law and Disciplinarity: Thinking Beyond Borders*, (Palgrave Macmillan US, 2003), 67-99.