INTERNATIONAL LAW STUDIES

Volume 87

International Law and the Changing Character of War

Raul A. "Pete" Pedrozo and Daria P. Wollschlaeger
Editors

Naval War College
Newport, Rhode Island
2011

IV

Low-Intensity Computer Network Attack and Self-Defense

Sean Watts*

I. Introduction

In May 2010, the United States Department of Defense activated the US Cyber Command,[1] consolidating leadership of six previously dispersed military organizations devoted to cyber operations.[2] To its supporters, Cyber Command represented a significant accomplishment as congressional misgivings over the command's mission, its effects on American citizens' privacy and ambiguous limits on its authority had delayed activation for nearly a year.[3]

These concerns featured prominently in the confirmation of Lieutenant General Keith Alexander, the President's nominee to lead Cyber Command. In written interrogatories, the Senate Armed Services Committee asked, "Is there a substantial mismatch between the ability of the United States to conduct operations in cyberspace and the level of development of policies governing such operations?"[4] General Alexander's response identified a gap "between our technical capabilities to conduct operations and the governing laws . . . ."[5] However, he later observed, "Given current operations, there are sufficient law, policy, and authorities to govern DOD cyberspace operations."[6]

* Associate Professor, Creighton University Law School; Assistant Department Chair, International & Operational Law Department, The Judge Advocate General's School, United States Army Reserve.

General Alexander's responses often struck such dissonant tones. And while his unclassified responses generally offered little legal reflection, he commented in detail on international self-defense law and cyber operations.[7] His responses portrayed existing law under the UN Charter as adequate to defend US interests from cyber attack. Further, he indicated the United States would evaluate threats and attacks in the cyber domain exactly as it would in other security realms.[8] Yet, the same section of responses noted a lack of international legal consensus concerning which cyber events violate the prohibition on the use of force or activate the right of self-defense, suggesting a less than coherent structure to this important international legal regime.[9]

Meanwhile, cyber attacks have rapidly migrated from the realm of tech-savvy doomsayers to the forefront of national security consciousness.[10] One need no longer be an experienced programmer or use much imagination to appreciate the threat posed by cyber attacks. Incidents such as the disruptions experienced in Estonia in 2007 and Georgia in 2008 provide concrete examples of practices, trends and potential harm posed by future cyber events.[11]

Similarly, cyber conflict theorists paint an increasingly lucid picture of the strategy and tactics that will inspire future attacks and shape defensive efforts. Cyber strategy is evolving rapidly, as threat capabilities and tactics shift to exploit newly discovered vulnerabilities. While defending against massive cyber catastrophes remains a priority for planners, a growing contingent of cyber theorists concludes that campaigns of diffuse, low-intensity attacks offer an increasingly effective strategy for cyber insurgents and State actors alike. Operating below both the focus of defensive schemes and the legal threshold of States' authority to respond with force, low-intensity cyber attacks may prove to be a future attack strategy of choice in cyberspace.

The confluence of Cyber Command's activation with publication of details of recent cyber incidents, as well as insight into emerging cyber strategy, provides an opportunity to critically evaluate General Alexander's assessment of the international law of self-defense as well as the overall significance of the events in Estonia and Georgia. Specifically, it is worthwhile to consider whether the bargain governing use of force reflected in the 1945 UN Charter is adequate for the threats facing States today and for the future of cyberspace. Put differently, will the letter of the Charter's use-of-force regime operate as an effective regulation of States' efforts to secure cyberspace from one another and from non-State threats?

This article argues that the above-mentioned developments in cyber conflict will greatly strain the existing self-defense legal regime and cast past computer network attacks (CNA), such as the Estonian and Georgian incidents, in a new light. First, gaps in the law's response structure will prove highly susceptible to

low-intensity cyber attacks, leaving victim States to chose between enduring damaging intrusions and disruptions or undertaking arguably unlawful unilateral responses. Second, and related, CNA will produce a significantly expanded cast of players, creating a complex and uncontrollable multipolar environment comprising far more States and non-State actors pursuing far more disparate interests than in previous security settings. CNA are unprecedented conflict levelers. CNA technology is inexpensive, easy to acquire and use, and capable of masking identity. CNA permit otherwise weak States and actors to challenge security hegemony at low economic and security cost. Ultimately, these developments will test States' commitment to the collective security arrangement of the Charter and its accompanying restraints on unilateral uses of force to a far greater extent than previously experienced.

Efforts to prevent or defeat massive, debilitating CNA surely warrant attention and resources. However, if such incidents represent aberrations from the majority of cyber hostilities, exclusive legal attention to such catastrophes is surely misplaced. Accounting for and addressing low-intensity CNA are equally—if not more—important to maintaining international order and a place for law in securing cyberspace.

The inquiry begins with a snapshot of the law governing resort to self-defense.

II. Self-Defense under the UN Charter

Legal accounts of self-defense doctrine vary greatly. Debates on preemptive and anticipatory self-defense,[12] collective self-defense,[13] armed retribution or reprisal,[14] and burdens of proof[15] remain highly contentious and relevant to CNA. At times it seems each examination of these self-defense subtopics generates as many aspects as authors. This section will focus on two distinct but related issues concerning the doctrine of self-defense: first, the relevance of the right of self-defense to interactions with non-State actors and, second, the threshold of "armed attack" which gives rise to the right to exercise self-defense. The unsettled and evolving nature of these issues will prevent a definitive account of either, yet will set the stage for an illustration of how low-intensity CNA may influence the development of each.

Self-Defense against Non-State Actors

The plainest and most widely accepted understanding of the UN Charter portrays self-defense as an exception to the nearly comprehensive ban on the use of force by States.[16] Article 2(4) forbids the threat or use of force by States in their international relations.[17] Meanwhile, Article 51 provides one of two enumerated

exceptions, permitting Member States to take measures in self-defense in response to "armed attack."[18] The relevance of the self-defense exception to interactions between States is obvious. If Article 2(4) regulates the use of force "in . . . international relations" and Article 51 is intended as a legal exception, then the event that most obviously activates the right is armed attack by other States, the only entities traditionally capable of conducting international relations under the Charter.[19]

Less clear, at least as a legal matter, is how, if at all, the self-defense exception applies to "armed attack" by non-State actors. Traditionally, law enforcement models, not directly influenced by the Charter, have guided State responses to non-State actors.[20] Yet current international and transnational security environments, shaped by a dramatic rise in the destructive capacity of violent non-State actors,[21] strongly suggest a role for self-defense beyond interactions between States.[22] While as a legal matter the UN Charter security regime is inapposite to State responses to non-State actors without links to State actors, such as attacks launched from *terra nullius* or international waters, such situations seem unlikely or at least exceedingly rare.[23] Far more prevalent are hostile activities by non-State actors based on or launched from UN Member States' sovereign territories, where the Charter's use-of-force regime operates clearly in theory if not so clearly in practice. A fractured and incomplete jurisprudence has emerged to cover the issue. Two International Court of Justice (ICJ) opinions address self-defense and non-State actors under the Charter.

Confronted by decades of attacks from outside its territory, Israel, in 2002, began work on a 450-mile barrier comprised alternately of concrete walls, fencing, wire and electronic sensors.[24] Encroaching on Palestinian territory, the barrier greatly restricted vehicle and pedestrian traffic. In its filings for the 2004 *Wall* advisory opinion, Israel justified construction of the wall on Palestinian territory as an exercise of self-defense under Article 51.[25] The argument was consistent with prior Israeli assertions to the General Assembly that self-defense included "the right of States to use force in self-defence against terrorist attacks."[26]

In a split decision, the Court rejected the Israeli claim. The Court asserted Article 51 had "no relevance" to interactions with non-State actors such as Palestine.[27] The advisory opinion is nearly summary in this regard, providing no interpretive support, citations to *travaux préparatoires* or examples of State practice. The Court also left unaddressed a point raised in Judge Higgins's separate opinion that the text of Article 51 does not include any indication "that self-defense is only available when armed attack is made by a State."[28] In his declaration, Judge Buergenthal expressed similar objection to the Court's opinion. He argued the Court gave inadequate weight to the fact the attacks originated outside Israeli borders, whatever the international legal status of that territory.[29]

Further criticism of the advisory opinion[30] focused on the Court's failure to consider State practice since adoption of the Charter.[31] States have routinely invoked self-defense doctrine, and Article 51 specifically, to justify the use of force against non-State actors. Several commentators have catalogued States' post-Charter resort to measures in self-defense against non-State actors, including actions taken by the United States, Israel, Portugal, Russia, Ethiopia and South Africa.[32] These accounts, and Security Council reactions thereto, paint a portrait of self-defense far more relevant to efforts against hostile non-State actors.[33]

The majority of State practice cited in opposition to the *Wall* Court's work showcases measures of self-defense alleging varying degrees of host-State support to the attacking non-State actor. Yet not all purported exercises of self-defense have included such links. In 1976, a series of South African intrusions into the territory of neighboring States to pursue non-State actors were distinct from other exercises in this important respect. South Africa asserted a right of self-defense absent such State involvement.[34] The South African government conceded that the States from which rebels operated were not complicit; however, it defended its territorial intrusions as justified in self-defense to continue its pursuit of rebel forces.[35] While the Security Council condemned[36] South Africa's acts and appeared to denounce the "hot pursuit"[37] theory of self-defense, disapproval may be attributable in greater part to the racist policies underlying these measures than to the legality of the theory itself.

Ultimately, the most convincing effort to reconcile the *Wall* Court's account of self-defense with its critics' competing claims emphasizes that the Israeli-Palestinian situation involved no transnational interactions. That is, owing to Palestine's failure to attain statehood, the *Wall* advisory opinion might be read not to reach the issue of valid State responses to non-State actors' armed attacks that originate from another State's territory. One might then plausibly cabin the opinion to situations not involving State actors or their territories, leaving open the issue of exercises of self-defense against non-State actors operating from sovereign territory. Yet the critique persists that a stronger analytical effort by the Court to identify the operative legal framework would have included an exploration of customary norms regulating the exercise of self-defense against purely non-State actors.

Only a year after the *Wall* advisory opinion, the ICJ had an opportunity to revisit and clarify the issue of transnational self-defense against non-State actors. In *Armed Activities on the Territory of the Congo*, Uganda defended its military operations against rebel groups operating from eastern Democratic Republic of the Congo (DRC).[38] Uganda offered two justifications for the attacks, both grounded in self-defense. First, it argued that DRC support for anti-Ugandan rebels triggered Uganda's right of self-defense, including the use of force on DRC territory. Second,

and alternatively, Uganda argued that the DRC's inability to control the territory from which anti-Ugandan rebels operated permitted Ugandan measures in self-defense on DRC territory.[39] Thus in some respects, the Ugandan claims were not unlike the earlier South African arguments rejected by the Security Council.

Surprisingly, the *Armed Activities* Court did not rule on the lawfulness of Uganda's self-defense against non-State actors. Instead, the Court declined to accept Uganda's characterization of the operations as defensive in nature, noting that the invasion far exceeded in scale and scope what would have been necessary to counter the rebel threat.[40] Curiously, the Court skipped over the traditional threshold analysis of whether the right to self-defense had been activated, reaching instead the issue of whether the use of force in question constituted a proportionate response. Thus the case left unaddressed the issue of States exercising self-defense in the context of transnational operations against non-State actors.

Once again, the Court attracted criticism for its failure to elaborate on the issue of self-defense against non-State actors.[41] In particular, critics argued the Court should have used the *Armed Activities* case to better explain how self-defense doctrine relates to issues of State responsibility generally. To some members of the Court, the opinion missed an opportunity to clarify the distinct but related standard of State responsibility for non-State actors' conduct within sovereign territory, a matter left uncertain by a prior decision but closely related to the exercise of self-defense.[42]

In 1986, the Court's *Nicaragua* judgment announced a standard for attributing non-State actors' conduct to States for purposes of self-defense.[43] The *Nicaragua* Court ruled that States exerting "effective control" over non-State actors launching armed attacks within or from their territories were subject to lawful measures in self-defense from victim States.[44] However, the *Nicaragua* effective control standard did not fare well in practice, leaving too much ambiguity to operate as a workable limit on States' exercise of self-defense.[45] Later, a separate UN-created court, the International Criminal Tribunal for the former Yugoslavia, offered a competing standard for State responsibility.[46] The *Armed Activities* judgment, however, did little to clarify or adapt the *Nicaragua* standard. The case offers no substantive clarity concerning the level of State support for hostile non-State actors that would give rise to a lawful exercise of self-defense by a victim State.

Critics of the *Armed Activities* decision also point to evidence of States' views on self-defense in response to non-State actors. Many regard the Security Council resolutions and the North Atlantic Treaty Organization (NATO) response to the 9/11 terrorist attacks on the United States as authoritative in this respect.[47] Unquestionably sufficient in intensity and effect to qualify as armed attacks,[48] the 9/11 attacks prompted both the Security Council and NATO explicitly to recite Charter-based

self-defense as a lawful response. Condemning the attacks as international terrorism, as well as threats to international peace and security, UN Security Council Resolutions 1368[49] and 1373[50] each reaffirmed the United States' right to exercise self-defense. Recalling efforts to muster Security Council support, William Howard Taft IV, then State Department Legal Adviser, recalls, "[We] had no difficulty in establishing that we had a right to use force in self-defense against Al-Qaeda and any government supporting it."[51] With similar dispatch, NATO invoked, for the first time, Article 5 of its organizing treaty with references to collective self-defense, as well as the UN Charter self-defense regime.[52] The legal effect of invoking Article 5 was to regard 9/11 as an attack upon all NATO member States.[53]

Clearer political statements in favor of applying self-defense doctrine to attacks by non-State actors are difficult to imagine. Scholars have seized on the 9/11 Security Council resolutions in particular as definitive State support for the exercise of self-defense under the Charter against non-State actors.[54]

Yet the legal import of the 9/11 political responses is debatable.[55] Security Council resolutions undoubtedly wield legal force. Under the Charter, States are bound to carry out the provisions of resolutions.[56] However, the extent to which they influence and shape legal doctrine or operate as independent legal precedent is questionable.[57] On one hand, Security Council voting presents States an opportunity to voice positions concerning resort to self-defense.[58] Discussion preceding votes on resolutions frequently generates detailed expression of *opinio juris* on issues concerning resort to self-defense.[59]

On the other hand, debate and voting are axiomatically political manifestations, reflecting economic, security and strategic self-interest as much as deliberate and principled legal thought. Use or threat of the veto by permanent members frequently prevents resolutions from reflecting comprehensive, majority State views on legal issues. Further undermining claims to status as law, Security Council practice with respect to self-defense lacks uniformity or regard for precedent. Examining Security Council self-defense practice, Professor Franck identified strong patterns of inconsistency.[60] Franck observes, "The actual practice of the UN organs has tended to be more calibrated, manifesting a situational ethic rather than doctrinaire consistency either prohibiting or permitting all [self-defense] actions."[61]

As promised, the picture of self-defense against non-State actors remains cloudy despite codified law, abundant State rhetoric and significant proliferation in attacks. The ICJ seized neither of two recent opportunities to elaborate on the conditions under which self-defense operates in States' interactions with non-State actors. Nor did the Court on either occasion see fit to account for widely recognized State practice in the area. Thus, a widening rift has become apparent between positive

law and the Court's work on the one hand and State practice on the other. Unfortunately, this ambiguity is not unique to the issue.

The Threshold of "Armed Attack"

The UN Charter identifies "armed attack" as the event which gives rise to Member States' right of self-defense.[62] Accounts of the Charter's diplomatic conference indicate the term provoked considerable back-channel maneuvering.[63] Although still subject to substantial interpretation, the term "armed attack" is thought to offer a comparative advantage over vague customary notions of self-defense. In the words of Professor Stone, "armed attack" at least limits reference to "an observable phenomenon against which [the victim State] reacts."[64]

The prevailing view characterizes armed attacks as a subset of violent acts within a broader grouping of acts that qualify as uses of force.[65] Though perhaps tempting, drawing precise parallels between the Article 2(4) prohibition on "use of force" and the Article 51 threshold of "armed attack" is flawed.[66] The modifier "armed" appears intended to eliminate lower levels of force from consideration. Mere coercion does not activate the right of self-defense,[67] if such activities even qualify as uses of force.[68] Classically understood, "armed attack" envisions uses of force producing destruction to property or lethal force against persons.[69] As Professor Stone asserts, the term also ensures a level of definition to prevent aggressors from fraudulently pleading self-defense to excuse offensive operations.[70] Graphically portrayed, one might imagine a Venn diagram with a large circle encompassing uses of force and a smaller circle within representing armed attacks. Thus, all armed attacks constitute uses of force, whereas not all uses of force rise to the level of armed attack.

Again, the ICJ has weighed in. In the *Nicaragua* case, the Court suggested the threshold of armed attack involved not merely destruction or invasion but also consideration of "scale and effects."[71] In addition to armed invasion by regular forces, the Court observed, "the sending by a State of armed bands to the territory of another State" to conduct similar armed activities would classify as an armed attack.[72] It is important to note that the Court did not examine instances where such bands carried out activities not involving arms or failing to produce destructive consequences usually associated with armed activity. Rather, the Court distinguished invasions from mere assistance "in the form of the provision of weapons or logistical or other support."[73] While conceding that such activities perhaps constituted a threat or use of force, perhaps implicating Article 2(4), the Court concluded routine logistical activities would generally not give rise to the right of self-defense.[74]

The practical significance of the Charter's—and the Court's—distinction between mere uses of force and more extreme armed attacks is a gap in response structure.[75] The plainest understanding of the distinction concludes that while States may respond to armed attacks with force, including armed measures of self-defense, States may not respond with armed violence or even force to mere uses of force. That is, the Charter's Article 2(4) general prohibition on the use of force by States continues to operate, even against States that have suffered an unlawful threat or use of force. Only armed attack frees a State from the prohibition on the use of force. In this respect, Article 51 operates as an incomplete exception to the prohibition on the use of force. The prevailing view holds that the Charter permits States to respond to mere uses of force only with measures of self-help not themselves rising to a use of force.[76] Thus the Charter reserves reciprocal uses of force in response to mere violations of Article 2(4) short of armed attack to the Security Council's response regime.[77]

While seemingly a sound textual interpretation, the gap has not aged well. Certainly, removing States' authority to respond with unilateral force to all but the most serious and violent events is in keeping with the spirit and intent of the Dumbarton Oaks drafting conference of 1945. Yet time and events have proved the Security Council unable to respond to many apparent violations of Article 2(4), leaving victims of acts falling within the gap either hostage to the flawed Security Council regime or faced with violating the letter and spirit of the Charter.[78] The gap proves particularly troubling to States underrepresented, either themselves or by allies, at the Security Council.

The recurring issue of so-called frontier incidents and self-defense illustrates well the contours of the ICJ's struggle to reconcile practice with text. Typically, frontier incidents are small-scale skirmishes of limited duration between States' armed forces. Christine Gray describes frontier incidents as "the most common form of force between States."[79] The ICJ has endorsed the legal concept of a frontier incident as falling short of "armed attack." In the same passage of the *Nicaragua* case cited above to describe the intensity element of "armed attack," the Court distinguished an armed attack from "a mere frontier incident."[80] Yet the Court offered almost no elaboration and did not revisit the issue in its factual examination of the parties' respective territorial violations. Critics of the frontier-incident distinction disparage its apparent toleration of "protracted and low-intensity conflict."[81] Still, there are signs that important State actors accept frontier incidents as part of the spectrum of uses of force outside armed attack and thus not giving rise to a broader exercise of self-defense, confirming the Charter's response gap.[82]

The gap theory is not a universally held view.[83] In a separate opinion to the *Oil Platforms* judgment, Judge Simma called the gap theory into question.[84] He posited

that lawful responses to armed force should generally track the acts that provoke them. While he agreed that only force amounting to armed attack opened the door to full-fledged self-defense, he argued that States are permitted to respond to force short of armed attack with "defensive military action 'short of' full-scale self-defence."[85] Rather than embrace the gap theory's all-or-nothing approach to defensive responses to force, Judge Simma advocated a spectrum of proportionality. In some ways like the Court's approach to the Ugandan operations in *Armed Activities*, Judge Simma would seemingly supplant the Charter's "armed attack" threshold with a floating scale of proportionality of action in States' international relations. It seems his standard is satisfied so long as a State's response to a use of force matches the intensity, scale and duration of the force suffered initially. Interestingly, a passage of the *Nicaragua* case seems to reinforce Judge Simma's view, supporting proportionate countermeasures in response to uses of force not amounting to armed attack.[86]

A further response to the gap attempts to shrink the conceptual space between the use of force and armed attack by simultaneously raising the threshold of acts qualifying as uses of force under Article 2(4), while lowering the bar for acts qualifying as armed attack under Article 51.[87] Returning to the previously imagined Venn diagram, this approach would shrink the circle representing use of force while expanding the circle representing armed attack. Such understandings minimize, if not eliminate, the situations in which States are unable to respond to uses of force unilaterally while greatly increasing the realm of situations in which they may employ force in self-defense.

The gap-shrinking effort and Judge Simma's approach may be useful as efforts to sustain the relevance of the Charter to modern international relations. Casual reviews of State practice seem to support them. Yet gap shrinking surely demands a better explanation of the distinct phrasing of the Charter's respective articles. And ultimately, in some sense, the gap-shrinking approach appears merely to shift interpretive debate back to the meaning of the term "armed attack."

In this way, gap shrinking makes no contribution to resolving the persistent ambiguities surrounding "armed attack," namely the intensity, duration and scope components of the term. And while Judge Simma's approach appeals to intuitive senses of equity and self-preservation, it is similarly difficult to reconcile with the letter of the Charter's concessions of sovereignty, no matter their practical flaws. Despite their utilitarian merits, neither approach is particularly satisfying as a matter of textual interpretation, setting up a conflict between principled interpretation and realistic practice in the law of self-defense.

Ultimately, perhaps even committed positivists must entertain a certain amount of sympathy for views that tolerate a broader range of coercive or forceful

responses from State victims of unlawful uses of force. New operational norms, not precisely consistent with the formal security regime of the Charter, may have emerged through subsequent State practice. It has been argued, "The Charter is not a commercial contract but a constitution."[88] But surely some level of determinism is appropriate, just as it is surely true that the bargain struck by States through the Charter reflected meaningful cessions of sovereignty.

Bearing in mind the contestable legal issues in self-defense, what is happening meanwhile in cyber conflict?

III. The Estonian and Georgian Incidents

Because of the highly classified nature of States' CNA practices and their past infrequency, the earliest legal analyses of CNA resorted to hypothetical or speculative events. Considering how few practical examples these writers had to work with, early forecasts of the operation of self-defense in CNA, if partly speculative, are nonetheless impressive.[89] Examples of CNA have since proliferated, providing ready grist for the mills of cyber security and cyber law analysts alike. Details of two recent events in particular, the 2007 Estonian and 2008 Georgian cyber incidents, have guided a great deal of discussion and policy.

Estonia 2007

In April of 2007, after relocating a Soviet-era World War II memorial from its prominent place in the capital city of Tallinn, Estonia suffered uncharacteristically violent protests by ethnic Russians.[90] Immediately afterward, a series of distributed denial of service (DDoS) attacks swept Estonian government and banking websites.[91] Lasting approximately one month, the DDoS[92] attacks prevented access to and defaced government websites and halted government e-mail traffic.[93] The DDoS attacks also interrupted Estonian Internet banking for portions of several business days.

The perpetrators of the DDoS attacks found a target-rich environment in Estonia. More than any other nation of its size, Estonia reflects an information systems society.[94] Wireless Internet, e-banking and web-based government services abound in Estonia. Internet access is available in a remarkable 98 percent of Estonian territory.[95] Home to the popular web-based voice call service Skype, Estonia boasts high rates of personal Internet usage and claims to have been the first country to conduct Internet elections.[96] Over 500,000 people, nearly half its citizens, have used government e-services.[97]

At its outset, the 2007 Estonian event generated strong emotional reactions. Estonian politicians immediately compared the incident to an invasion and to

conventional military activity.[98] However, quickly after the true nature of the incident became apparent, Estonian authorities realized that by accepted metrics the event did not amount to armed attack. Although widespread within Estonia and of nearly a month's duration, the event produced chiefly economic and communications disruptions. Public confidence in government and electronic services likely suffered as well, but certainly not on the scale or in the nature anticipated by armed attack. Additionally, because the DDoS attacks transited as many as 178 countries,[99] Estonia never traced responsibility for the events to another State, despite lingering suspicion of Russian government involvement.[100] In the final analysis, Estonia attributed the disruptions to patriotic teams of ethnic Russian hackers, only loosely affiliated with one another.[101]

The Estonian response seems to confirm that an armed attack did not occur as well. Estonian countermeasures were entirely passive in nature. Estonian technicians replied largely by expanding network bandwidth to diffuse the effects of the DDoS attacks.[102] The government focused its later responses on criminal investigations and also developing its domestic penal law to better account for cyber terrorism and intrusions.[103] Estonia seems at no point to have given serious thought to resorting to measures of self-defense under either the Charter or the NATO Washington Treaty.[104] Nor, given its difficulties attributing the attacks, does it seem it could have.

The Estonian cyber incident undoubtedly sounded an alarm for the international community. But while the event provoked calls for cooperative cyber forensics and criminal law enforcement, very little of the incident generated lessons or insights with respect to self-defense. Legal analyses conclude almost unanimously that the event did not give rise to the right of self-defense.[105] Only a year later, a similar incident would sound the same alarm and inspire comparable discussion, yet would immediately shed no greater light on self-defense and CNA.

Georgia 2008

Although in a de facto sense independent since 1991, the Caucasus region of South Ossetia has remained all the while part of the Republic of Georgia in a legal sense. In 2008, after an increase in Ossetian separatist activity, Georgia attempted to reassert control of the region.[106] These operations provoked a swift and militarily decisive intervention by Russian air and armored forces.[107]

Before the physical invasion, Georgian government websites suffered a series of DDoS attacks.[108] The Georgian presidential website was out of service for more than 24 hours, then experienced manipulation including defacement of the President's image.[109] By the date of the Russian physical invasion, websites belonging to the Ministry of Foreign Affairs, Ministry of Defense, the National Bank and several

Georgian news outlets had already suffered DDoS attacks.[110] The day following the invasion, Georgia's largest bank was also struck. All told, the DDoS operations continued for nearly a month, long outlasting kinetic hostilities and even postdating a ceasefire.[111]

In terms of information technology, Georgia was no Estonia. In fact, the relatively underdeveloped Georgian information infrastructure may have mitigated the impact, economic and otherwise, of the incident.[112] While Georgia's highly concentrated distribution nodes simplified the attackers' task, Georgians did not rely heavily on government web-based or e-services. The greatest impact of the incident appears to have been reputational and related to restricting information flow between the government and its citizens during the invasion crisis.[113]

For purposes of characterizing the Georgian cyber incident as an armed attack, coincidence with the Russian physical invasion complicates legal analysis. The incident preceded, or more likely constituted part of, a conventional military invasion that undoubtedly qualified as an armed attack.[114] Yet isolated from the succeeding kinetic measures, the cyber aspects of the Georgian incident were of minimal scope and intensity. At its worst, the cyber incident disrupted banking activities and limited communications between the Georgian government and the population. No loss of life, physical injury or destruction of property was directly attributable to the cyber operations. Perhaps the most interesting legal issues arising from the Georgian cyber incident concern timing of self-defense and whether the cyber disruptions could have been interpreted as an indication of imminent armed attack.

But the conclusions one can draw regarding the exercise of self-defense in the realm of pure cyber operations are limited. Similar to the Estonian episode, Georgia never identified conclusive evidence of Russian government responsibility for conduct of the disruptions. Also, the cyber incidents alone do not seem to have risen to the level of armed attack. Had the physical invasion not followed, the Georgian cyber incidents would likely have left Georgia in much the same place as 2007 Estonia: inconvenienced (though comparatively less so), vulnerable, angry and embarrassed. And while, at first impression, neither incident appears useful to elaborate on the details of self-defense doctrine, each may be a useful foreboding of future trends in CNA likely at some point to implicate self-defense.

While neither incident reached the threshold of armed attack, the costs of each in terms of security seem real. Classifying these events as mere communications disruptions or interference seems not to capture the function and importance of computer networks in the information age.[115] If the Estonian and Georgian DDoS attacks did not cripple either State or produce damage to property or persons, they certainly reduced public confidence and exposed critical vulnerabilities. The chaos

and confusion of the Georgian cyber attacks may even have facilitated or set favorable conditions for Russian physical attacks. After these incidents, one might fairly ask whether failure to produce physical damage or injury really justifies placing these incidents on the lower end of a conflict spectrum and whether such events are aberrations or indications of the future of cyber conflict. One might also seriously ask whether more powerful States would have exercised similar restraint.

IV. Low-Intensity Cyber Strategy

A growing strand of cyber scholarship suggests the Estonian and Georgian incidents are harbingers of future cyber conflict. Within a broader spectrum of cyber attack, strategists highlight low-intensity cyber warfare as an increasingly prevalent and threatening form of conflict. By exploiting intrinsic tactical advantages, as well as weaknesses in Western military thinking, low-intensity CNA have great potential to abuse narrowly conceived models of conflict to the advantage of cyber insurgencies and States. Failing to perceive and treat the threats posed by low-intensity attacks hampers targets' long-term security and plays into the hands of the attacker. This section briefly explains how such attacks not only exploit tactical and strategic advantages but may also leverage the legal gaps identified previously.

Military doctrine commonly uses a conflict spectrum keyed to levels of violence.[116] Along the cyber variant of the spectrum, low-intensity CNA distinguish themselves from their high-intensity counterparts in two important respects. First, low-intensity CNA add a dimension of concealment not apparent in high-intensity CNA. Specifically, in addition to masking the identity of the attacker, low-intensity CNA conceal their effects. They accomplish this largely through restraint in scale and scope. In the attacker's ideal scenario, the victim of low-intensity CNA is unaware of the damage to the target system. In other words, successful low-intensity CNA never awaken a sleeping giant.

Low-intensity CNA also differ from the majority of high-intensity CNA in their ability to frustrate correlation. In the event they *are* detected, successful low-intensity CNA should appear to the victim as unrelated or isolated events.[117] Selecting varied targets, spreading effects and timing attacks in apparently random sequences prevent the target from perceiving the larger-scale, more threateningly coordinated effort of the attacker. Inability to correlate reduces the likelihood of response by the victim, despite cumulative reductions in capacity and efficiency. The analogy to the "death by a thousand cuts" is apt.[118]

In addition to being distinct from other CNA, low-intensity CNA are tactically and strategically attractive for several reasons. Tactically, low-intensity CNA are less likely to provoke debilitating responses from targets. Because the target is often

unaware the attack has happened at all, low-intensity CNA may provoke no response. Even if the victim becomes aware of the attack's effect, the isolated damage may be so limited that a response is simply not worthwhile. As a kinetic counterexample, the immense scale of the Al-Qaeda 9/11 attacks forfeited this tactical advantage, greatly compromising the organization's long-term capacity.[119] Operating below the target's response threshold, low-intensity attacks avoid this blunder, simultaneously enjoying relative impunity and preserving the utility of the attacker's cyber tools for future operations.

Strategically, low-intensity CNA may also prove a wise effort. Low-visibility, low-intensity CNA may be effective to retard a target's economic, social and technological development. Such developmental constraint might easily yield long-term payouts in strategic competition. In a struggle for technological and military supremacy, even a slight advantage in efficiency or conversion capability may prove decisive.[120]

Low-intensity CNA are also highly feasible. In general, cyber operations are often far less expensive than traditional military operations.[121] The technology required is widely available and relies to a great extent on automation rather than personnel.[122] Low-intensity CNA compound these advantages that CNA enjoy as a general matter. As one theorist observes, "You can do a simple attack against a lot of computers. Or you can do a sophisticated attack against a few computers. But it is really hard to do a sophisticated attack against a lot of computers, especially an attack that would achieve a meaningful military objective."[123]

Further enhancing feasibility, low-intensity CNA permit incorporation of unaffiliated or even unsophisticated actors. Non-State actors such as cyber militias increasingly populate cyberspace, offering services for profit or political sympathy.[124] Enlistment may be as simple as offering a personal computer, Internet access and a web browser.[125] "Hacktivist" involvement in low-intensity CNA not only diffuses effects but also strengthens efforts to launder the sponsor's identity as the source of attack.[126] A victim might easily misinterpret well-masked hacktivist attacks as unrelated acts of vandalism rather than a concerted effort to degrade capacity or security.

In addition to these very practical advantages, advocates of low-intensity CNA base their arguments on flaws in military theory. Modern Western military thought has long rested on bifurcations of peace and war, notions of military and civilian separation.[127] Classic military theory reserves military action to escalations of hostile conduct between parties above recognized thresholds of violence.[128] Military legal disciplines reinforce the war-peace and military-civilian distinctions. The law governing the conduct of hostilities, or *jus in bello*, captures the military-civilian bifurcation through the targeting principle of distinction.[129] Similarly, the

law of war reflects the war-peace distinction through pervasive chapeau or application threshold provisions as prerequisites to operation of the law.[130] The vast majority of the positive *jus in bello* only operates in armed conflict between States. Recalling the *jus ad bellum* outlined in section I, one detects a similar bipolar assumption with respect to hostilities and self-defense. Under the Charter regime, either armed attack has occurred, unleashing the use of force, or something short of armed attack has occurred, restricting responses to peaceful means short of force.

Cyber theorists contrast these Western traditions with notions of conflict that understand military action as part of a general and continuous strategic competition between powers rather than as an exception to peace.[131] If Western powers regard as legally extinct Clausewitz's characterization of war as a continuation of politics, competing views continue to carry Clausewitz's torch. Consistent with this tradition, work by two Chinese People's Liberation Army officers urges an appreciation of an unrestricted understanding of warfare extending into informational, commercial, currency and media realms.[132]

Cyber conflict theorists argue that Western military thought's blind spot for unconventional and low-intensity hostilities renders States susceptible to abuse. Failing to perceive pinprick attacks as part of an enemy's expanded conception of conflict frustrates correlation and delays defensive efforts. Actors acquainted with States' military response thresholds and willing to extend their activities into traditionally civilian realms, such as strategic communication, currency exchange, trade and media, gain crucial strategic and tactical advantages. Low-intensity CNA are ideally suited to pursuing such advantages.

Finally, low-intensity CNA are attractive because they leverage seams in developed States' national security response structures. Particularly if directed at private enterprise, low-intensity CNA may successfully evade government computer network defenses. Moreover, private sector victims may not report attacks to public sector authorities to preserve investor and consumer confidence. Industries concerned with maintaining client privacy or trade secrets may be especially inclined to underreport low-intensity CNA.

The operational environment of cyberspace may not be the only incentive to low-intensity non-State actors' tactics. The law may incentivize such operations as well. Cyber operations just below the "use of force" threshold or even in the space between "use of force" and "armed attack" become attractive considering views that limit States' lawful responses to the latter. The *Wall* advisory opinion's view that self-defense is irrelevant to attacks by non-State actors surely fosters a sense of impunity or insulation from retribution or response. For example, one might imagine a protracted and diffuse campaign of cyber frontier incidents, designed to

harass and frustrate a target but also designed to remain below the legal threshold for measures in self-defense. If economic, communications and psychological effects, no matter how profound, don't trigger the right to respond with force, much less the armed attack threshold for use of self-defense, CNA seem a particularly apt means for imposing such effects to harm or at least harass and weaken States. This is especially the case if the strict legal view that limits the use of force to "armed attack" holds true.

In the end, coupled with emerging cyber doctrine, the Estonian and Georgian incidents might take on important new meaning. The arguments for low-intensity, low-impact cyber operations suggest they may no longer be the realm of criminals and economic saboteurs but rather deliberate strategies to influence the international security environment. Informed by a broader conception of cyber strategy and conflict theory, the Estonian and Georgian incidents might indeed mean something more to States and implicate self-defense and security in ways not obvious at the time of each, with important implications for the Charter's doctrine of self-defense. States may no longer be able to afford to treat such incidents as mere criminal acts or communications disruptions. States may very well look to measures in self-defense as a response to such events, notwithstanding their failure to comport with traditional understandings of "armed attack." The implications for the future of the UN Charter self-defense regime may be grim.

V. Conclusion: The Impact of Low-Intensity CNA on the Self-Defense Legal Regime

Scholars have built impressive careers predicting the demise of the Charter's security regime.[133] In 1970, Professor Thomas Franck argued that the Article 2(4) use of force regime mocked States from its grave.[134] He asserted that new forms of attack made the notions of war on which the Charter was based obsolete, while State practice eroded States' mutual confidence in the system.[135] Addressing self-defense, Franck presciently identified wars too small and wars too large to fit within Article 51.[136] Ultimately, Franck indicted incongruence between the norms of the international security system and the national interests of States as the perpetrator of his imagined legicide[137]—perhaps the very same concerns that motivated the Senate's question to General Alexander.[138]

So, are the laws regulating resort to force, and specifically self-defense, out of synch with planned cyber capabilities and strategies? Or more precisely, does the Charter's self-defense doctrine leave States adequate authority to respond to the full range of CNA threats they face?

The answer depends, in large part, on the version of self-defense one adopts. As section II demonstrated, despite a universally adopted codification and decades of jurisprudence and State practice, the doctrine of self-defense remains highly indeterminate. If General Alexander expressed satisfaction with the state of the law, his was likely a confidence grounded in a very broad and permissive understanding of the doctrine. Informed by views that regard the Charter's response gap skeptically or seek to define it away, one might indeed express satisfaction with the range of responses available to State victims of CNA. Espousing a similar view, the US State Department Legal Adviser recently offered a vote of confidence in self-defense doctrine as it relates to lethal overseas counterterrorism efforts.[139]

Yet such permissive views of self-defense suffer the textual shortcomings of their forebears.[140] Christine Gray asserts that States rarely speak of self-defense in purely legal terms.[141] Her evaluation is difficult to square with claims that in the post-Charter world States defend nearly all uses of force as self-defense.[142] Yet the future may prove Gray's observation increasingly accurate. Recent State expressions appear particularly vague and open-textured, grounded in notions of instinct, rights of survival and natural law rather than positivist models of conflict regulation.[143] Increasingly, it seems States have resurrected pre-Charter notions that self-defense includes all means necessary for self-preservation against all threats. Practice is offered to the exclusion of positivist expressions of law, rather than as a vehicle for elucidating or understanding it. Even committed international law sovereigntists must detect discomfiting, pre-Charter realist tones.

On the other hand, if one adopts the narrower view of self-defense, including the apparent textual response gap between use of force and armed attack, the general's proffered mismatch between law and capacity may indeed be real. Particularly with respect to low-intensity CNA, State victims appear hostage to law that would deny resort to proportionate countermeasures and restrict effective action to a security regime paralyzed by politics.

What emerges appears to be a choice of threats. Either one accepts a real threat to the positive *jus ad bellum*'s claim to law, or one accepts very real threats to States' security as a trade-off for preserving legal idealism. Neither reflects well on the future of the law. Each constitutes a mismatch in its own sense.

If past predictions of the demise of the Charter's security regime, such as Franck's, have proved exaggerated,[144] low-intensity CNA may vindicate them yet. As Franck's critics point out, the international security environment of the twentieth century likely profited from the Charter's limits through undetectable instances of restraint.[145] The argument claims the Charter regularly influenced decisions to refrain from resort to force but unlike decisions to use force, restraint leaves little in

the way of observable evidence. Yet the prospect of low-intensity CNA is likely to change the calculus of these decisions.

With these cheap, anonymous and effective weapons, States find a greatly altered international security game. The low barriers to entry into CNA, and particularly low-intensity CNA, greatly increase the number of potential players.[146] Just in terms of frequency of occurrence, the number of instances in which States will be called upon to evaluate whether resort to force or measures in self-defense is justified or necessary increases.

Further, as the Estonian and Georgian episodes still suggest to many, non-State actors may be effective proxies for States in CNA. It appears non-State actors will be a persistent feature of future CNA. And for non-State actors operating on their own behalf, modern hostilities offer few levelers on the order of CNA. CNA are tremendous force multipliers and are abundantly available. Low-intensity CNA offer the potential for catastrophic effects against asymmetrically developed and resourced States. Conversely, many non-State actors are simply retaliation- and even deterrence-proof, offering defenders little in the way of targets.

Thus, low-intensity CNA not only increase the population of attackers but also the pool of potential defenders. This is true in two senses. First, as the Georgian event shows, even States with rudimentary information systems capacity present ripe targets for CNA. More States present themselves as potential targets of hostile acts, increasing in absolute terms the opportunity and likelihood that hostilities will erupt. Second, more States are likely to participate themselves in CNA for the same reasons that more non-State actors are. Thus in a CNA security environment, more States will possess means to respond to attacks or, more important, to events short of armed attack yet sufficiently disruptive or annoying to provoke a hostile response.

On a related note, and equally disruptive to restraint in the exercise of self-defense, CNA may permit more States to "go it alone." As a more attainable means of self-defense, CNA may free States from reliance on collective security arrangements. In contrast to the twentieth century's bipolar security environment, CNA's low barriers to entry may lead to a multipolar system of lone actors. Decisions whether to resort to self-defense will lack the temperance and restraint that collective security arrangements have offered. Thus, low-intensity CNA may topple preexisting vertical arrangements of States into a level or horizontal array of power.

Finally, CNA rearrange the cast of actors in the security environment in a more literal way. CNA render geography largely meaningless. States previously insulated from armed attack by distance or terrain enjoy no such benefits in cyberspace. Borders and neighbors do not determine one's cyber security. Rather, in an ironic

sense, susceptibility to attack may be a function of the extent to which a State relies on the very information technology that is targeted. As information systems proliferate the target environment becomes richer, increasing the frequency with which States must make decisions about exercising self-defense.

The preceding factors suggest critical consequences for the viability of self-defense doctrine. As low-intensity CNA increase the pool of defenders, attackers and targets, opportunities for disparate or even idiosyncratic views or approaches to self-defense will also proliferate. Low-intensity CNA will generate conflicting accounts of self-defense doctrine with respect to applicability to non-State actors and the "armed attack" threshold, as well as other issues such as anticipatory and collective self-defense. It is ominously clear that the phenomena that prompted Franck to pronounce the death of the Charter security regime are not merely also present in CNA; they are present in far greater degrees.

Few of the developments, legal or technical, outlined in this article portend a stable or effective international self-defense regime. Rather than evince satisfaction with the bargain struck in 1945, emerging views on self-defense, such as that expressed by General Alexander, likely reflect altered understandings of limits on States' freedom of action. The effects on the integrity and viability of the law of self-defense are compounded if one extrapolates the opportunity to interpret and apply self-defense doctrine to the vast cast of actors, State and non-State, in cyberspace. While surely motivated in part by legitimate perceptions of very real threats, these views are highly susceptible to producing a chaotic, dangerous and multipolar security environment. Faced with the daunting prospect of persistent low-intensity CNA, ruling views on self-defense may quickly become in fact entirely untethered from the Charter's security regime. Understood in light of emerging low-intensity CNA doctrine, the Estonian and Georgian events become highly relevant to the development of self-defense law. One can easily imagine, and might already conjure, a law of self-defense that resorts to the Charter's regime in name only, revealing it to have been as Stone posited, one of many "vain attempts to abolish power."[147]

Notes

1. Initial orders to create the command date to mid-2009. *See* Ellen Nakashima, *Gates Creates Cyber-Defense Command*, WASHINGTON POST, June 24, 2009, at A08, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/06/23/AR2009062303492.html. Appropriately enough, information on Cyber Command, often referred to as CYBERCOM, is available from a US Department of Defense website. *See* http://www.defense.gov/home/features/2010/0410_cybersec (last visited Sept. 20, 2010).

2. William J. Lynn III, *Introducing U.S. Cyber Command*, WALL STREET JOURNAL, June 3, 2010, § A, at 15, *available at* http://online.wsj.com/article/SB10001424052748704875604575280881128276448.html.

3. Ellen Nakashima, *Cyber Command Chief Says Military Computer Networks Are Vulnerable to Attack; U.S. military networks in war zones could be targeted, Alexander says*, WASHINGTON POST, June 4, 2010, at A02, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/06/03/AR2010060302355.html.

4. Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command 9 (on file with author) [hereinafter General Alexander Advance Questions]. *See Nominations of VADM James A. Winnefeld, Jr., USN, to be Admiral and Commander, U.S. Northern Command/Commander, North American Aerospace Defense Command; and LTG Keith B. Alexander, USA, to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command: Hearing Before the S. Comm. on Armed Services*, 111th Cong. (2010), http://armed-services.senate.gov/testimony.cfm?wit_id=9367&id=4505.

5. General Alexander Advance Questions, *supra* note 4, at 9.

6. *Id.* One might easily imagine, especially considering General Alexander's additional position as Director of the National Security Agency, that his response had in mind domestic legal limitations as much as international law.

7. *Id.* at 11–12.

8. *Id.* at 12.

9. *Id.* at 11. General Alexander submitted a portion of his response on the topic of international law on the use of force in a classified supplement. *See id*.

10. *See* Bill Lambrecht, *U.S. is Busy Thwarting Cyber Terrorism*, LATIMES.COM (June 24, 2010), http://www.latimes.com/business/la-fi-cyber-terrorism-20100624,0,3306751.story. Early in the current president's tenure, cyber security took a prominent place in national security strategy. *See* The White House, Cyberspace Policy Review (2009), *available at* http://www.whitehouse.gov/administration/eop/nsc/cybersecurity.

11. *See infra* section III.

12. *See* David Sadoff, *A Question of Determinacy: The Legal Status of Anticipatory Self-Defense*, 40 GEORGETOWN JOURNAL OF INTERNATIONAL LAW 523 (2009) (concluding no legal consensus exists on anticipatory self-defense); W. Michael Reisman & Andrea Armstrong, *The Past and Future of the Claim of Preemptive Self-Defense*, 100 AMERICAN JOURNAL OF INTERNATIONAL LAW 525 (2006) (predicting the possibility of future invocations of preemptive self-defense); Sean D. Murphy, *The Doctrine of Preemptive Self-Defense*, 50 VILLANOVA LAW REVIEW 699 (2005) (identifying methodological differences as the source of divergence in international lawyers' disagreements over preemptive self-defense); Thomas M. Franck, *Preemption, Prevention and Anticipatory Self-Defense: New Law Regarding Recourse to Force?*, 27 HASTINGS INTERNATIONAL AND COMPARATIVE LAW REVIEW 425 (2004) (advocating abandonment of preemptive self-defense as inconsistent with the UN Charter).

13. *See* Carsten Stahn, *Collective Security and Self-Defense after the September 11 Attacks*, 10 TILBURG FOREIGN LAW REVIEW 10 (2002); George K. Walker, *Anticipatory Collective Self-Defense in the Charter Era: What the Treaties Have Said*, 31 CORNELL INTERNATIONAL LAW JOURNAL 321 (1998); Hans Kelsen, *Collective Security and Collective Self-Defense under the Charter of the United Nations*, 42 AMERICAN JOURNAL OF INTERNATIONAL LAW 783 (1948).

14. *See* Roberto Barsotti, *Armed Reprisal*, *in* THE CURRENT LEGAL REGULATION OF THE USE OF FORCE 79 (Antonio Cassese ed., 1986) (identifying "radical change" in the doctrine of self-defense as regards resort to armed reprisal); Michael A. Newton, *Reconsidering Reprisals*, 20

DUKE JOURNAL OF COMPARATIVE & INTERNATIONAL LAW 361 (2010) (arguing that a refined doctrine of reprisal might produce clearer limiting criteria than strained resorts to self-defense).

15. *See* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶¶ 67–77 (Nov. 6) (rejecting US justification for use of force as self-defense on failure to meet burden of proof); Geoffrey Corn & Dennis Gyllensporre, *International Legality, the Use of Military Force, and Burdens of Persuasion: Self-Defense, the Initiation of Hostilities, and the Impact of the Choice between Two Evils on the Perception of International Legitimacy*, 30 PACE LAW REVIEW 484 (2010) (identifying incentive structures resulting from comparative burdens of proof required of self-defense versus collective security action).

16. Professor Dinstein is perhaps best known for this characterization of self-defense. *See* YORAM DINSTEIN, WAR, AGGRESSION & SELF-DEFENCE (4th ed. 2005). *See also* ANTHONY CLARK AREND & ROBERT J. BECK, INTERNATIONAL LAW AND THE USE OF FORCE 31 (1993). Professor Dinstein observes, "Only when the universal liberty to go to war was eliminated, could self-defence emerge as a right of signal importance in international law." DINSTEIN, *supra* at 177. A competing characterization asserts that the right of self-defense preceded the UN Charter use-of-force regime and thus stands as an autonomous legal right rather than an exception. *See* MYRES S. MCDOUGAL & FLORENTINO P. FELICIANO, LAW AND MINIMUM WORLD PUBLIC ORDER: THE LEGAL REGULATION OF INTERNATIONAL COERCION 217–20, 232–41 (1961); JULIUS STONE, AGGRESSION AND WORLD ORDER 99–101 (1958) (identifying "absurdities" through extreme examples of a strict reading of Article 51); Sean D. Murphy, *Self-Defense and the Israeli* Wall *Opinion: An* Ipse Dixit *from the Court?*, 99 AMERICAN JOURNAL OF INTERNATIONAL LAW 62, 64 (2005) (emphasizing that the Charter includes an "*inherent*" right of self-defense) (emphasis in original). The United States' understanding of self-defense also appears to emphasize the inherent rather than exceptional nature of self-defense under international law. US Navy, US Marine Corps & US Coast Guard, The Commander's Handbook on the Law of Naval Operations NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A, 4-4–4-5 (2007) [hereinafter Commander's Handbook] (citing Chairman of the Joint Chiefs of Staff Instruction 3121.01B, Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces (2005)).

17. U.N. Charter art. 2, para. 4

18. *Id.*, art. 51. Articles 39 and 42, in conjunction, form the second exception to the Article 2(4) prohibition, permitting States to use force when authorized by the Security Council.

19. *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 57–58 (7th ed. 2008) (admitting, however, the possibility of limited international personality for some international organizations); 1 INTERNATIONAL LAW: BEING THE COLLECTED PAPERS OF HERSCH LAUTERPACHT 136–37 (Elihu Lauterpacht ed., 1970).

20. Indeed, the 9/11 terror attacks on the United States provoked a significant legislative effort to strengthen domestic law enforcement. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001); Claude d'Estree & Luke Andrew Busby, *U.S. Response to the Events of September 11, 2001: The USA PATRIOT Act, Title III*, *in* LAW IN THE WAR ON INTERNATIONAL TERRORISM 107 (Ved P. Nanda ed., 2005) (analyzing and forecasting consequences of the Act).

21. *See* John Arquilla, *The New Rules of War*, FOREIGN POLICY, Mar./Apr. 2010, at 60, *available at* http://www.foreignpolicy.com/articles/2010/02/22/the_new_rules_of_war (Arquilla observes, "[T]errorists and transnational criminals have embraced connectivity to coordinate global operations in ways that simply were not possible in the past. Before the Internet and the

World Wide Web, a terrorist network operating cohesively in more than 60 countries could not have existed. Today, a world full of Umar Farouk Abdulmutallabs awaits—and not all of them will fail.").

22. LINDSAY MOIR, REAPPRAISING THE RESORT TO FORCE: INTERNATIONAL LAW, *JUS AD BELLUM,* AND THE WAR ON TERROR 150 (2010) (noting the novelty of the Taliban/Al-Qaeda relationship, where "the government of a State had apparently been inferior to, or dependent upon, a terrorist organization within its territory").

23. However, international shipping and naval forces have suffered increased attacks by Somali pirates in the western Indian Ocean. *See Piracy at Sea*, NYTIMES.COM, http://topics.nytimes.com/top/reference/timestopics/subjects/p/piracy_at_sea/index.html?scp=2&sq=somalia%20pirates&st=cse (last updated Nov. 10, 2010) (noting a record number of pirate attacks in 2009); Borzou Daragahi & Edmund Sanders, *Pirates Show Range and Daring*, LATIMES.COM (Nov. 18, 2008), http://articles.latimes.com/2008/nov/18/world/fg-piracy18.

24. *See* Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 80 (July 9) [hereinafter Legal Consequences of the Construction of a Wall]. Israel has since removed portions of the wall in response to improving security. *See* Sheera Frenkel, *Israel Removes Wall, Palestinians Remain Wary*, NPR.COM (Aug. 18, 2010), http://www.npr.org/templates/story/story.php?storyId=129279814.

25. Legal Consequences of the Construction of a Wall, *supra* note 24, ¶¶ 138–39.

26. *Id.*, ¶ 138 (citing U.N. Doc. A/ES-10/PV.21 at 6 (Oct. 20, 2003)).

27. *Id.*, ¶ 139.

28. *Id.*, ¶ 33 (separate opinion of Judge Higgins).

29. *Id.*, ¶ 6 (declaration of Judge Buergenthal).

30. *See* Murphy, *supra* note 16, at 62 (describing the opinion as "startling in its brevity and, upon analysis, unsatisfactory"); Ruth Wedgwood, *The ICJ Advisory Opinion on the Israeli Security Fence and the Limits of Self-Defense*, 99 AMERICAN JOURNAL OF INTERNATIONAL LAW 52, 58 (2005). *But see* Iain Scobbie, *Words My Mother Never Taught Me—"In Defense of the International Court,"* 99 AMERICAN JOURNAL OF INTERNATIONAL LAW 76, 77 (2005) (regarding the opinion's statements on self-defense as "well-founded").

31. Murphy, *supra* note 16, at 67–70.

32. MOIR, *supra* note 22, at 140–47. CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 136 (3d ed. 2008).

33. *See* Murphy, *supra* note 16, at 67.

34. GRAY, *supra* note 32, at 137 (citing SC 1944th meeting (1976)).

35. *Id.*

36. S.C. Res. 568, ¶¶ 1, 4, U.N. Doc. S/RES/568 (June 21, 1985).

37. *See* Commander's Handbook, *supra* note 16, at 3-10 (permitting US Navy vessels to exercise authority beyond territorial waters where pursuit is initiated in internal waters).

38. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 1 (Dec. 19) [hereinafter Armed Activities].

39. *See* Phoebe N. Okowa, *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, 55 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 742, 747–48 (2006) (citing Position of the High Command of Uganda on the Presence of the Uganda Peoples Defence Forces in the DRC (Sept. 11, 1998). Counter-Memorial of the Government of Uganda, vol. I, annex 27 & ch. 3 (Apr. 21, 2001)).

40. Armed Activities, *supra* note 38, ¶ 147. The Court identified "no need to respond to the contentions of the Parties as to whether and under what conditions contemporary international law provides for a right of self-defence against large-scale attacks by irregular forces." *Id.*

Reinforcing its skepticism of the Ugandan self-defense claim, the Court added, "The Court cannot fail to observe, however, that the taking of airports and towns many hundreds of kilometres from Uganda's border would not seem proportionate to the series of transborder attacks it claimed had given rise to the right of self-defence, nor to be necessary to that end." *Id.*

41. Okowa, *supra* note 39, at 749; Stephanie A. Barbour & Zoe A. Salzman, *"The Tangled Web": The Right of Self-Defense against Non-State Actors in the* Armed Activities *Case*, 40 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 53 (2007) (concluding the *Armed Activities* case left an understanding of self-defense ill-prepared for threats posed by non-State actors in control of State territory).

42. Armed Activities, *supra* note 38, ¶ 8 (separate opinion of Judge Simma).

43. Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 195 (June 27). It should be noted that for jurisdictional reasons, the *Nicaragua* Court analyzed the customary rather than purely-Charter-based body of law.

44. *Id.*

45. *See* Christopher J. Le Mon, *Unilateral Intervention by Invitation in Civil Wars: The Effective Control Test Tested*, 35 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 741 (2003) (charting operation of the effective control test as a limit on State interventions).

46. Although not addressing self-defense specifically, the International Criminal Tribunal for the former Yugoslavia developed an alternative standard for State responsibility in the 1999 *Tadic* case. Prosecutor v. Tadic, Case No. IT-94-1-A, Judgment, ¶ 120 (Int'l Crim. Trib. for the former Yugoslavia July 15, 1999) (determining that to attribute actions of rebels to a State "it is sufficient that the group as a whole be under the *overall control* of a State") (emphasis added).

47. *See* DINSTEIN, *supra* note 16, at 207–8; Christian J. Tams, *The Use of Force against Terrorists*, 20 EUROPEAN JOURNAL OF INTERNATIONAL LAW 359, 377 (2009).

48. *See* NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT (2004).

49. S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sept. 12, 2001).

50. S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

51. William Howard Taft IV, *The Bush (43rd) Administration*, *in* SHAPING FOREIGN POLICY IN TIMES OF CRISIS: THE ROLE OF INTERNATIONAL LAW AND THE STATE DEPARTMENT LEGAL ADVISER 127, 128–29 (Michael P. Scharf & Paul R. Williams eds., 2010).

52. Press Release, North Atlantic Treaty Organization, Statement by the North Atlantic Council (Sept. 12, 2001), *available at* http://www.nato.int/docu/pr/2001/p01-124e.htm.

53. North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243, *available at* http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

54. *See* DINSTEIN, *supra* note 16, at 207–8; Barbour & Salzman, *supra* note 41, at 65 (noting that Resolutions 1368 and 1373 compound uncertainty whether non-State actors can rise to the level of armed attack).

55. GRAY, *supra* note 32, at 18–20.

56. U.N. Charter art. 25.

57. Even ICJ decisions only bind parties to the case. *See* Statute of the International Court of Justice art. 59, June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 993. Louis Sohn has written impressively on the issue of which and how UN agents should interpret the Charter. Louis B. Sohn, *The UN System as Authoritative Interpreter of Its Law*, *in* 1 UNITED NATIONS LEGAL ORDER 169 (Oskar Schachter & Christopher C. Joyner eds., 1995).

58. U.N. Charter art. 31 (permitting non-members of the Security Council to participate in discussions where the latter considers their interests to be "specially affected").

59. *See, e.g.*, THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 676 n.141 (Bruno Simma et al. eds., 1995) (recounting Security Council debate of the lawfulness of Israeli strikes initiating the 1967 Six-Day War) [hereinafter UN CHARTER COMMENTARY].

60. THOMAS FRANCK, RECOURSE TO FORCE 77 (2002) (surveying UN Security Council reactions to use of force in self-defense by Belgium, Turkey, Israel and, on six separate occasions, the United States).

61. *Id.*

62. U.N. Charter art. 51. Scholars generally recognize two schools of thought on the threshold of self-defense: a narrow understanding, viewing "armed attack" as the exclusive trigger for the right of self-defense, and a broad understanding, viewing "armed attack" as but one of many events capable of justifying resort to self-defense. *See* Natalino Ronzitti, *The Expanding Law of Self-Defense*, 11 JOURNAL OF CONFLICT AND SECURITY LAW 343, 344–45 (2006); Norman M. Feder, *Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack*, 19 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 395, 403–4 (1987) (evaluating both views and advocating the narrow variant).

63. Professor Brownlie notes that the records of the San Francisco diplomatic conference include no explanation of the term "armed attack." IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 279 (1963). However, a historical account of the creation of the United Nations provides some background and parole evidence. *See* STEPHEN C. SCHLESINGER, ACT OF CREATION: THE FOUNDING OF THE UNITED NATIONS 181–83 (2003) (offering a narrative account of diplomatic efforts to draft Article 51).

64. STONE, *supra* note 16, at 72.

65. *See* UN CHARTER COMMENTARY, *supra* note 59, at 663 n.11 (citing exclusively German-language authors).

66. *See id.* at 663 ("It is to be emphasized that Arts. 51 and 2(4) do not exactly correspond to one another in scope, i.e.[,] not every use of force contrary to Art. 2(4) may be responded to with armed self-defence").

67. The records of the Charter's drafting conference suggest strongly that economic coercion would also not qualify as a use of force. *See* UN CHARTER COMMENTARY, *supra* note 59, at 112 (noting States' rejection of a Brazilian proposal to include economic coercion within the scope of the Article 2(4) prohibition).

68. *See* STONE, *supra* note 16, at 72 n.168 (quoting Netherlands delegate M. Röling).

69. *See* Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 934 (1999).

70. STONE, *supra* note 16, at 72.

71. Military and Paramilitary Activities, *supra* note 43, ¶ 195.

72. *Id.* The Court relied on the General Assembly's Definition of Aggression in significant part. *Id.* (relying on G.A. Res. 3314 (XXIX), U.N. Doc. A/RES/3314 (Dec. 14, 1974)).

73. *Id.*

74. *Id.* With respect to these findings, Gray observes, "The Court gave no authority for this Statement and was criticized for its failure to do so by some commentators." CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 143 (2d ed. 2004).

75. *See* UN CHARTER COMMENTARY, *supra* note 59, at 664.

76. *See* DINSTEIN, *supra* note 16, at 193–96 (confirming the gap theory of the Charter's response structure); BROWNLIE, *supra* note 63, at 279 (observing, "Indirect aggression and the incursions of armed bands can be countered by measures of defence which do not involve military operations across frontiers"). For discussion of the topic in the context of CNA specifically, see

THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 47–49 (2000); Schmitt, *supra* note 69, at 929 (observing that only CNA intended to directly cause physical destruction or injury authorize forcible responses under the Charter).

77. Further support for the gap theory may be found in the International Court of Justice *Nicaragua* and *Oil Platforms* cases. *See* DINSTEIN, *supra* note 16, at 193–94; Military and Paramilitary Activities, *supra* note 43, ¶ 191; Oil Platforms, *supra* note 15, ¶ 51.

78. *See* David J. Scheffer, *Commentary on Collective Security*, *in* LAW AND FORCE IN THE NEW INTERNATIONAL ORDER 101–4 (Lori Fisler Damrosch & David J. Scheffer eds., 1991) [hereinafter Damrosch & Scheffer].

79. GRAY, *supra* note 32, at 177.

80. *See* discussion *supra* p. 66 (citing Military and Paramilitary Activities, *supra* note 43, ¶ 195).

81. *See* W. Michael Reisman, *Allocating Competences to Use Coercion in the Post–Cold War World*, *in* Damrosch & Scheffer, *supra* note 78, at 39.

82. *See* GRAY, *supra* note 32, at 181 (citing William Howard Taft IV, *Self-Defense and the Oil Platforms Decision*, 29 YALE JOURNAL OF INTERNATIONAL LAW 295, 302 (2004)).

83. Taft, *supra* note 82, at 295.

84. Oil Platforms, *supra* note 15, ¶ 12 (separate opinion of Judge Simma). I am grateful to Professor Wolff Heintschel von Heinegg for alerting an audience to this passage at a recent international law symposium.

85. *Id.*

86. *See* Military and Paramilitary Activities, *supra* note 43, ¶ 249. Curiously, however, the Court restricted forcible countermeasures to the victim State, ruling out collective use thereof. *Id.*

87. *See* UN CHARTER COMMENTARY, *supra* note 59, at 664 (citing Julius Stone, *Force and the Charter in the Seventies*, 2 SYRACUSE JOURNAL OF INTERNATIONAL LAW AND COMMERCE 1, 11–12 (1974); ALFRED VERDROSS & BRUNO SIMMA, UNIVERSELLES VÖLKERRECHT: THEORIE UND PRAXIS ¶ 472 (3d ed. 1984)).

88. Reisman, *supra* note 81, at 43.

89. *See, e.g.*, WALTER GARY SHARP, CYBERSPACE AND THE USE OF FORCE (1999); WINGFIELD, *supra* note 76; Eric Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STANFORD JOURNAL OF INTERNATIONAL LAW 207 (2002); Schmitt, *supra* note 69 (developing the most influential model for assessing the legal significance of cyber events).

90. For an excellent account of the Estonian incident, see ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 14–25 (2010) [hereinafter TIKK ET AL.].

91. *See id.* at 20.

92. DDoS describes the use of masses of bogus access requests to websites to flood communications channels, inducing shutdown. *See* Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 63, 70 (2010).

93. *See* TIKK ET AL., *supra* note 90, at 20–21, 24–25.

94. *See id.* at 16–18.

95. *See id.* at 17.

96. *See id.* at 17–18 (citing *Estonia First Country in the World to Introduce Internet Voting*, EURACTIV, http://www.euractiv.com/en/egovernment/estonia-country-world-introduce-internet-voting/article-145735 (last updated June 15, 2007)).

97. *See* TIKK ET AL., *supra* note 90, at 18.

98. Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia: Parliament, ministries, banks, media targeted: Nato experts sent in to strengthen defences*, GUARDIAN (London), May 17, 2007, Home Pages at 1, *available at* http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

99. Charles Clover, *Kremlin-backed Group Behind Estonia Cyber Blitz*, FT.COM (Mar. 11, 2009), http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html.

100. Noah Schactman, *Kremlin Kids: We Launched the Estonian Cyber War*, WIRED (Mar. 11, 2009), http://blog.wired.com/defense/2009/03/pro-kremlin-gro.html. An Internet security consultant speculates the Russian government employed an organization known as the Russian Business Network (RBN) to carry out the attacks on its behalf in exchange for immunity for prior criminal acts. *See* Linton Chiswick, *Cyber Attack Casts New Light on Georgia Invasion*, THE FIRST POST (Aug. 15, 2008), http://www.thefirstpost.co.uk/45135,features,cyber-attack-casts-new-light-on-georgia-invasion. The consultant describes the RBN as

> a shadowy, St Petersburg–based internet company . . . believed to provide secure hosting for much of the world's online crime, from illicit pornography to credit card fraud and phishing. It is also believed to control the world's biggest and most powerful "botnet"—a network of infected zombie computers of a scale necessary to perform destructive cyber-terrorism or cyber-warfare on an entire State.

Id.

101. *See* TIKK ET AL., *supra* note 90, at 23.

102. *See id.* at 24.

103. *See id.* at 26–29.

104. *Id.* at 25–26.

105. *See id.*

106. *See id.*

107. *See* Michael Schwirtz, Anne Barnard & C. J. Chivers, *Russia and Georgia Clash Over Separatist Region*, NYTIMES.COM (Aug. 8, 2008), http://www.nytimes.com/2008/08/09/world/europe/09georgia.html?hp (offering a same-day account of the invasion); Peter Finn, *A Two-Sided Descent Into Full-Scale War*, WASHINGTON POST, Aug. 17, 2008, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/08/16/AR2008081600502_pf.html (offering expanded, day-by-day accounts of events leading up to and the conduct of the invasion).

108. *See* TIKK ET AL., *supra* note 90, at 70; John Markoff, *Before the Gunfire, Cyberattacks*, NEW YORK TIMES, Aug. 13, 2008, at A1.

109. *See* TIKK ET AL., *supra* note 90, at 70.

110. *See id.* at 70–72.

111. *See id.*

112. *See id.* at 78.

113. *See id.*

114. Not surprisingly, Russia defended the invasion as an exercise of self-defense to address Georgian maltreatment of Russian citizens in South Ossetia. Yet under the traditional view, only one side may lawfully claim self-defense. As Dinstein suggests, "There is no self-defence from self-defence." DINSTEIN, *supra* note 16, at 178.

115. *See* ALVIN TOFFLER, THE THIRD WAVE (1984) (describing transition from an industrial-centric to an information-centric age).

116. Headquarters, Department of the Army, FM 3-0, Operations, at 2-2 (2008) (describing situations of increasing violence, including stable peace, unstable peace, insurgency and general war).

117. Antoine Lemay, José M. Fernandeza & Scott Knight, *Pinprick attacks, a lesser included case?*, *in* CONFERENCE ON CYBER CONFLICT, PROCEEDINGS 2010, at 183, 191 (Christian Czosseck & Karlis Podins eds., 2010) [hereinafter Lemay et al.].

118. *See id.* at 190.

119. Gustavo De Las Casas, *Destroying al-Qaeda Is Not an Option (Yet)*, FOREIGN POLICY.COM (Nov. 10, 2009), http://www.foreignpolicy.com/articles/2009/11/10/the_case_for_keeping_al_qaeda?page=0,0 (noting that since 2001 40 percent of Al-Qaeda leadership has been killed or captured).

120. *See* Lemay et al., *supra* note 117, at 190. Lemay and his co-authors describe conversion capability as the ability of a State to transform strategic resources, such as knowledge and money, into military advantage, usually through a military-industrial complex. *Id.*

121. *See* TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 2-2 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009).

122. *See id.*

123. *See* Samuel Liles, *Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency*, *in* CONFERENCE ON CYBER CONFLICT, *supra* note 117, at 47, 53 (quoting BRUCE D. BERKOWITZ, THE NEW FACE OF WAR: HOW WAR WILL BE FOUGHT IN THE 21ST CENTURY 147 (2003)).

124. *See* Rain Ottis, *From Pitchforks to Laptops: Volunteers in Cyber Conflicts*, *in* CONFERENCE ON CYBER CONFLICT, *supra* note 117, at 97.

125. *See id.*

126. One wonders, however, whether unorganized or undisciplined hacktivists might compromise the relative advantage of denying the target correlation through overly enthusiastic attacks.

127. DAVID A. BELL, THE FIRST TOTAL WAR 24–25 (2007) (noting the eighteenth-century advent of a Western conceptual separation of military and civilian).

128. Lemay et al., *supra* note 117, at 188.

129. *See* LAW OF WAR HANDBOOK 166 (Keith E. Puls ed., 2005) (this publication of the US Army's Judge Advocate General's School describes distinction as the "grandfather of all principles" of the law of war).

130. *See, e.g.*, Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 2, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 2, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Convention Relative to the Treatment of Prisoners of War art. 2, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Convention Relative to the Protection of Civilian Persons in Time of War art. 2, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287; Convention No. II with Respect to the Laws and Customs of War on Land art. 2, July 29, 1899, 32 Stat. 1803, 1 Bevans 247.

131. *See* Lemay et al., *supra* note 117, at 189; Liles, *supra* note 123, at 48–49.

132. QIAO LIANG & WANG XIANGSUI, UNRESTRICTED WARFARE (1999).

133. Thomas Franck, *Who Killed Article 2(4)?*, 64 AMERICAN JOURNAL OF INTERNATIONAL LAW 809 (1970).

134. *Id.* at 809.

135. *Id.*

136. *Id.* at 812.

137. *Id.* at 836.

138. *See supra* p. 59.

139. Harold Hongju Koh, Legal Adviser, US Department of State, Remarks at the Annual Meeting of the American Society of International Law: The Obama Administration and International Law (Mar. 25, 2010), http://www.state.gov/s/l/releases/remarks/139119.htm.

140. *See supra* pp. 68–69.

141. GRAY, *supra* note 32, at 28.

142. *See* DINSTEIN, *supra* note 16, at 178; WINGFIELD, *supra* note 76, at 40–41; UN CHARTER COMMENTARY, *supra* note 59, at 663.

143. *See* Koh, *supra* note 139 (reciting the inherent right to self-defense to justify targeting of terror suspects). In a recently published account of his experience as State Department Legal Adviser, Abraham Sofaer observes that no US president has ever accepted or is ever likely to accept a restrictive view of the right to self-defense. Sofaer explicitly rejects the notion "that a State may exercise its right of self-defense only if the 'attack' is carried out by another State and occurs on the territory of the State claiming the right to defend itself." Abraham Sofaer, *The Reagan and Bush Administrations*, *in* SHAPING FOREIGN POLICY IN TIMES OF CRISIS, *supra* note 51, at 55, 83.

144. *See* Louis Henkin, *The Reports of the Death of Article 2(4) Are Greatly Exaggerated*, 65 AMERICAN JOURNAL OF INTERNATIONAL LAW 544 (1971).

145. *See id*.

146. *See* Ottis, *supra* note 124, at 99–101.

147. STONE, *supra* note 16, at 104 (characterizing ambiguity of resort to force terminology as evidence of limits of legal efforts to curb States' pursuit of self-interest in international relations).