Cyberwarfare: Attribution, Preemption, and National Self Defense

By John Dever* and James Dever**

I. INTRODUCTION

In recent years, both the capability to protect against a large-scale cyberattack, and the capability to launch a successful cyberattack against another country have become an integral and ever-growing part of the

---

* John P. Dever Jr. holds a L.L.M. in National Security Law from Georgetown University. He is the Global Crisis Management Leader at GE. He was also an Assistant U.S. Attorney, and prior to that, he was Assistant General Counsel in the Federal Bureau of Investigation's National Security Law Branch, Counterterrorism Division. He began his career as a U.S. Army Judge Advocate. He has served multiple combat deployments and is the recipient of the Bronze Star and the Purple Heart Medals.

** James A. Dever, Esq. holds an advanced degree in History and has worked with the Department of Homeland Security. He teaches at Quinnipiac University and is the General Counsel for a government contracting firm. He is a Judge Advocate in the U.S. Army Reserves.

national security strategy of the United States.[1] While conventional kinetic military attacks are likely to remain a mainstay of conflict for the foreseeable future, cyberattacks are rapidly becoming an attractive option as technology becomes both more sophisticated and widely accessible. This means of attack also permits a less powerful enemy, in the traditional sense of force on force engagements, to damage a stronger foe. In a fashion, it is the ultimate development in asymmetric warfare. The difficulty associated with attribution in a cyberattack makes this option ever more appealing as it is less likely to be met with a quick and deadly kinetic response. In essence, cyberspace may become a relatively safe haven from which to launch attacks.[2] The *2010 National Security Strategy* emphasized that "cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."[3] As the technology to engage in cyberattack proliferates, as appears inevitable, more actors, nations states, their proxies, non-state actors, criminal entities, and lone wolves will likely avail

---

[1] WHITEHOUSE, NATIONAL SECURITY STRATEGY 27 (2010), *available at:* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf [hereinafter, 2010 NATIONAL SECURITY STRATEGY]; U.S. DEP'T OF DEFENSE, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 4, *available at:* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf; WHITEHOUSE, WHITEHOUSE INTERNATIONAL STRATEGY FOR CYBERSPACE 12 (2011), *available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf* [hereinafter 2011 INTERNATIONAL STRATEGY FOR CYBERSPACE].

[2] LIEUTENANT COLONEL SCOTT W. BEIDLEMAN, DEFINING AND DETERRING CYBER WAR 21, *available at:* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA500795.

[3] 2010 NATIONAL SECURITY STRATEGY, *supra* note 2 at 27.

themselves of this technology, thereby increasing the threat picture to the United States.[4] These cyberattacks may eventually have a disproportionate impact, allowing those who seek to harm the United States destructive ability without the advanced weapons systems they would have once needed. [5]

The importance of cybersecurity to the United States was highlighted in the *2010 National Security Strategy*, where it was emphasized that protecting U.S. national security requires that the "U.S. military continues to have the necessary capabilities across all domains—land, air, sea, space, and cyber."[6] The *2010 National Security Strategy* highlighted the importance of cybersecurity to U.S. national security as a whole, and laid the foundations for the development of the *Department of Defense Strategy for Operating in Cyberspace*, and the *May 2011 Whitehouse International Strategy for Cyberspace*, which further emphasize the importance of cybersecurity.[7] In particular, the *May 2011 Whitehouse International Strategy for Cyberspace* advocates that "states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace,"[8] and that "[w]hen warranted, the United States will respond to hostile acts in cyberspace as [it]

---

[4] JAMES ANDREW LEWIS, CYBER ATTACKS, REAL OR IMAGINED, AND CYBER WAR, http://csis.org/publication/cyber-attacks-real-or-imagined-and-cyber-war,

[5] U.S. DEP'T OF DEFENSE, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 3 (2011), *available at:* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf. [hereinafter 2011 DEPARTMENT OF DEFENSE CYBERSPACE STRATEGY].

[6],2010 NATIONAL SECURITY STRATEGY, *supra* note 2 at 22

[7] 2011 DEPARTMENT OF DEFENSE CYBERSPACE STRATEGY, *supra* note 6 at 4; 2011 INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 2 at 12.

[8] 2011 INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 2 at 10.

would to any other threat to our country," including the use of military force.[9]

Despite the emphasis on the importance of cybersecurity in policy documents, there has been little discussion about when a cyberattack on the U.S. or conducted by the U.S. on another country becomes more than just interference in another country's affairs, and reaches the level of an armed attack that can be responded to in self-defense.[10] Indeed, the law of cyberattacks still retains the frameworks and tests applicable to traditional warfare. Such frameworks, however, using concepts such as "armed force" or "aggression" are inadequate analogies to address the nuances of cyber attacks. Therefore, this paper proposes a new consequentialist standard based on an "Effects Test" to define when cyberattacks constitute an armed attack that can be responded to in self-defense. This paper will also address the use of anticipatory self-defense in the cyber context by proposing a modification of the traditional *Caroline* doctrine using a court system as a check on abuse of the anticipatory self-defense doctrine.

II. CYBERATTACKS

In order to determine what legal regime should be used to combat cyberattacks, it is important to understand the many forms they take. One of the most difficult aspects of defining cyberattacks is the large amount of diversity among those acts that can be considered cyberattacks. A cyberattack broadly encompasses "the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident

---

[9] *Id.* at 14.

[10] *Id.* at 9 (discussing that new international norms are needed in the cybersecurity context but not stating what that new norms might be).

in or transiting these systems or networks."[11] In addition, the nature and seriousness of a cyberattack can vary based on the actors involved, the way in which the attack is conducted, what the result of the attack is.[12] Cyberattacks can include something as small as an individual hacking into the computer of another individual to obtain the person's banking information, or something as large scale as one country taking control of another country's military computers and firing that country's weapons, and all the possible activity that falls in between.[13]

III. CURRENT LEGAL FRAMEWORK

Determining when a cyberattack constitutes an armed attack is important in three contexts within the U.N. Charter framework, the first of which is a legal question, whereas the other two are policy questions that would need to be determined by the U.N. Security Council. First, it is important in determining whether an act will constitute an armed attack that a country can respond to in self-defense, second it is important in determining whether a cyberattack constitutes a threat to the peace, breach of the peace, or an act of aggression under Article 39, and third it is important in determining whether a cyberattack, when used by the Security Council to respond to a threat to the peace, breach of the peace, or an act of aggression, should be classified only as the use of force allowed under Article 42, or an action that does not constitute the use of force under Article 41. While the first context is perhaps the most important because it establishes a legal framework, but the second

---

[11] KENNETH W. DAM, ET AL., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 80 (2009).
[12] Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 422 (2011).
[13] *Id.* at 422-23.

two contexts demonstrate the power that the U.N. Security Council has to make decisions concerning various types of actions, whether an individual state can respond to that action, or whether the United Nations as a whole can respond. While two of the contexts involve a policy decision being made, instead of a legal decision, the guidance that can be provided through the definition of an armed attack can be useful in helping the Security Council make those policy decisions, and therefore limit the confusion among states about what is permissible with regards to cyberattacks.

A. ARTICLE 2(4) AND ARTICLE 51

The first context in which it is necessary to determine whether a cyberattack constitutes the use of force is with regards to the prohibition of the use of force. Under Article 2(4) of the U.N. Charter, "[a]ll 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."[14] This provides for a general prohibition on a country using physical force on another country, and therefore it is necessary to determine whether a cyberattack constitutes the use of force to determine whether any type of cyberattack is permissible under the U.N. Charter. Due to large variety in size and scope of cyberattacks, it is unlikely that every cyberattack would be considered to be the use of force, but the difficulty is in determining where to draw the line. For instance, stealing someone's personal information would be considered a cyberattack, but would not be considered to be the use of force. Within the U.N. Charter there is only one exception to the prohibition on the use of force established by Article

[14] U.N. Charter art. 2, para. 4.

2(4), and that is the right of self-defense under Article 51.[15] Article 51 states that:

> 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. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[16]

The right to self-defense is not unlimited under Article 51 because to act in self-defense, one must have been subjected to an armed attack.[17] The question then becomes what is an armed attack. What constitutes an armed attack is not specifically defined within the U.N. Charter, but the International Court of Justice (ICJ) has explored this issue in a few of its decisions.[18] In the Nicaragua case, the ICJ determined that it is necessary to distinguish between the gravest forms of the use of

---

[15] U.N. Charter art. 2, para. 4, art. 51.
[16] U.N. Charter art. 51.
[17] *Id.*
[18] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.)*, 1986 I.C.J. 14, ¶¶ 191, 210-211 (June 27); Oil Platforms (Islamic Republic of Iran vs. U.S.), 2003 I.C.J. 161, ¶¶ 51, 64 (November 6).

force, those constituting an armed attack, and other less grave forms.[19] While the use of force is allowed when responding in self-defense to an armed attack, the use of force is not allowed when merely responding to another state's intervention that does not reach the level of an armed attack.[20] The same principles were reiterated in the Oil Platform case, in which the court found that the actions of the Iranians did not rise to the level of an armed attack, and therefore the U.S. had no right to respond with force in self-defense.[21] While ICJ guidance on these issues is somewhat ambiguous, it is clear that it has held that the right to respond in self-defense is allowed in response to all forms of the use of force, but only the use of force that is considered to be an armed attack.[22] Within the cybersecurity context, this is a difficult distinction to draw.

B. ARTICLE 39

The second context in which it is necessary to determine whether a cyberattack constitutes an armed attack, is when determining whether a given action constitutes a threat to the peace, breach of the peace, or an act of aggression under Article 39.[23] Under Article 39 of the U.N. Charter,

> [t]he Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to

---

[19] *Nicaragua*, 1986 I.C.J. 14, at ¶ 191.
[20] *Id.* at ¶ 210-211.
[21] *Oil Platforms*, 2003 I.C.J. 161 at ¶¶ 51, 64.
[22] *Nicaragua*, 1986 I.C.J. 14, at ¶¶ 210-211; *Oil Platforms*, 2003 I.C.J. 161, at ¶¶ 51, 64.
[23] U.N. Charter art. 39.

> maintain or restore international peace and security."[24]

While the U.N. Charter allows for the U.N. Security Council to declare whether a specific act constitutes a threat to the peace, breach of the peace, or an act of aggression, there are no definitions of these specific terms in the Charter itself, and it is left up to the U.N. Security Council to determine both what these terms mean, and whether a particular action fits into one of these categories.[25] Therefore, what actions constitute a threat to the peace, a breach of the peace, or an act of aggression constitutes a policy decision by the Security Council.[26] The failure to have clear definitions makes it difficult for states to determine whether their actions are allowed by the Security Council prior to actually committing the actions. This is particularly true in the context of an emerging field, such as cyberspace. Having a definition that defines what would be an act of aggression within the cyberspace context would help states to ensure that they do not engage in these types of activities, and prevent conflict. In U.N. Resolution 3341, the General Assembly defined aggression as "the first use of armed force by a State in contravention with the Charter…although the Security Council may…conclude that a determination that a act of aggression has been committed would not be justified in the light of other relevant circumstances."[27] Resolution 3341 then goes on to list a number of possible actions that might constitute an act of aggression, and all of these examples include the use of armed force.[28] The

---

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] G.A. Res. 3314 (XXIX), U.N. GAOR, 29th Session (December 14, 1974).
[28] *Id.*

issue of what constitutes an act of aggression was revisited at the Kampala Review Conference of the Rome Statute in 2010, and Article 8 of the Rome Statute was amended to include a definition of what constitutes an act of aggression under the Rome Statute, and again requires the use of armed force.[29] Under both the U.N. General Assembly and the Rome Statute's definition of an act of aggression, an act of aggression requires the use of some sort of armed force, which results in complications in the cyberspace context because straightforward analogies cannot be made to any of the examples of the use of force provided.[30]

Although the determination about whether a cyberattack constitutes an act of aggression under Article 39 is a policy decision by the Security Council it would provide greater clarity in the international context if there were a more clearly defined standard, which separates in a distinct manner armed attack, aggression, and use of force.[31]

C. ARTICLE 41 AND 42

The third context in which it is necessary to determine whether a cyberattack constitutes an armed attack, is when the U.N. Security Council is deciding how to respond to a threat to the peace, breach of the peace, or an act of aggression, and if they decide to respond with a cyberattack, whether this action would be a response under Article 41 or Article 42 of the U.N. Charter.[32] Article 41 provides the Security Council with the ability to conduct measures not involving the use of

---

[29] Rome Statute of the International Criminal Court art. 8, July 17, 1998, 2187 U.N.T.S. 90.
[30] G.A. Res. 3314 (XXIX), U.N. GAOR, 29th Session (December 14, 1974); Rome Statute of the International Criminal Court art. 8, July 17, 1998, 2187 U.N.T.S. 90.
[31] U.N. Charter art. 39.
[32] U.N. Charter art. 41-42.

armed force, whereas Article 42 provides the Security Council with the ability to conduct measures using armed force when the measures under Article 41 would be inadequate or have proved to be inadequate.[33] Because of the variety in size and scope of the possible cyberattacks that could be conducted to respond to a threat to the peace, breach of the peace or an act of aggression, it would be impossible to put cyberattacks solely within Article 41 and 42, but also very difficult to determine where to draw the line as to which types of cyberattacks would be considered measures under Article 41 and which would be considered measures under Article 42.[34]

These three contexts in which the concept of an armed attack arises within the U.N. framework highlights the need for an alternative framework to handle cyberattacks because cyberattacks struggle to fit within the these frameworks in a meaningful way that can account for the diversity in the size and scopes of possible cyber attacks. In addition, it seems that under the current framework cyberattacks would very rarely constitute an armed attack or even an act of aggression because they do not appear to cross the ICJ's admittedly less than clear threshold of use of force or aggression, and because they do not usually involve armed forces in the conventional senses, and because it is difficult to make an analogy between cyberattacks that do not actually involve the use of weapons, and conventional acts that involve armed forces. Due to the fact that the current standards are difficult to apply in the cyberspace context in a meaningful way it is necessary to explore different possible frameworks to define when a cyberattack constitutes an armed attack that a country may respond to with self-defense.

---

[33] *Id.*
[34] *Id.*

IV. PROPOSAL FOR A NEW LEGAL FRAMEWORK, THE EFFECTS TEST

While there are those who believe that the current framework can be interpreted in ways that include cyberattacks, it seems clear that the current framework really does not take into account the broad spectrum of actions that can constitute a cyberattack, and limits those actions that might constitute an armed attack to a very small number. In response to the issues highlighted by the current framework, the Effects Test has been developed as the proposed alternative approach to looking at whether a cyberattack is an armed attack.[35] This test is intended to be broad enough to be able to more effectively analyze a wider variety of cyberattacks, while still limiting the number of cyberattacks that would be considered armed attacks. Under the Effects Test, a cyberattack is an armed attack if its consequences are those which would also be seen in a conventional attack.[36] This is evaluated based on several factors, including (1) the severity of the harm caused, (2) the immediacy of the effects, (3) the directness of the effects, (4) the invasiveness of the act that caused the attack, (5) the measurability of the consequences of the attack, and (6) the presumptive legitimacy of the actions taken that caused the harm.[37] By looking at the effects of the cyberattack in the context of these six factors, one can then determine which actions constitute an armed attack based on which action has effects that are similar

---

[35] COMMITTEE ON OFFENSIVE INFORMATION WARFARE, NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 33-34 (2009); Waxman, *supra*, n. 13 at 431–32.

[36] Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914 (1999).

[37] *Id.* at 914-15.

to those normally seen in an armed attack, yet with no armed forces present.[38]

V. The *Caroline* Doctrine

When addressing the issue of when the United States may respond to a cyberattack it is useful to consider historical antecedents of self-defense and consider how they would apply to the cyberattack arena. Specifically, a study of the *Caroline* case shows that a modification to the "necessity" prong of the *Caroline* test may be necessary in the cyberattack arena. Unlike the Bush Doctrine with its emphasis on preemption, a modernized *Caroline* test creates an anticipatory self-defense model that would rely heavily upon the advancement of technological capability to assist with the ever-vexing issue of attribution in the cyberattack arena. Much more attention would have to be paid to the concept of "probing" attacks, and whether such activity amounts to small scale attacks that may be compiled together and responded to with greater force.

The term "anticipatory self-defense" in the context of international law and *jus ad bellum* is commonly defined as a nation's ability to foresee the consequences of a given threat and to take proactive measures aimed at preventing those consequences.[39] Accordingly, anticipatory self-defense is distinguished from armed reprisal in that the former is protective while the latter is retributive.[40] Moreover, some legal scholars employ a further temporal analysis to differentiate between anticipatory self-defense and preemptive action. In this schema, preemptive action is where State A uses force to quell a possibility of future attack by State B even in those instances where there is no reason for State

---

[38] *Id.*

[39] Lucy Martinez, *September 11th, Iraq and the Doctrine of Anticipatory Self-Defense,* 72 UMKC L. REV. 123, 125 (2003).

[40] *Id.*

A to believe an attack by State B is planned and when no prior attack has occurred.[41] Meanwhile, anticipatory self-defense is understood as a narrower doctrine because State A must expect an imminent attack from State B.[42]

The *Caroline* incident was a dispute between the United States and the British Empire that occurred during the Canadian Rebellion of 1837.[43] The Canadian Rebellion was comprised of two regional conflicts that pitted disaffected French-Canadian smallholders against their landlords in Quebec as well as recent American immigrants to Canada against the British landed gentry in the western province of Ontario.[44] Many Americans who lived near the Canadian border sympathized with the plight of the rebels and located their struggle in terms of a second independence movement on the North American continent.[45] Yet despite the wellspring of popular support for the rebels in New York, the rebellion was defeated militarily when a poorly armed force of

---

[41] *Id.* at 125, 26.
[42] *Id.*
[43] Timothy Kearley, *Raising the Caroline,* 17 WIS . INT'L L. J. 323, 328 (1999).
[44] MICHAEL W. DOYLE, STRIKING FIRST: PREEMPTION AND PREVENTION IN INTERNATIONAL CONFLICT 11 (2008). This compilation of six essays contains an extended introduction by Dr. Stephen Macedo, Director of the Princeton University Center for Human Values, two essays by Doyle, three chapters by prominent legal authorities such as Dean Harold Hongju Koh who comment on Dr. Doyle's articulation of anticipatory self-defense, and a final rejoinder from Dr. Doyle's responses to his colleagues. The book explores these issues in a dynamic and dialectic way for a more pragmatic (less ideological) and nuanced development of the arguments.
[45] Kearley, *supra* note 44, at 328.

several hundred men were vanquished by a larger group of British militia and thereby failed to capture Toronto.[46]

Subsequent to the British victory in Ontario, rebel leader William Mackenzie fled across the border to New York where he canvassed support for a continuation of the rebellion to include procuring arms and recruiting young American and Canadian men for a "Patriot Army."[47] As one contemporary American intoned, volunteers flocked to Mackenzie's banner because "[o]nce the colonies of Great Britain, these states rebelled against her power and our fathers achieved our independence. We have considered it our boon and our birth-right to sympathize with, and fight for the oppressed. . . . The elements of revolution were ripening in the Canadas."[48] Accordingly, because the *Caroline* incident occurred during the Canadian Rebellion, it is perhaps more historically accurate to locate the event in terms of ordinary rather than anticipatory self-defense. Nonetheless, for better or worse, the process of politicization oftentimes drives collective interpretation of an event and for that reason because contemporaries understood the *Caroline* incident in terms of anticipatory self-defense, it stands for that historical proposition.

On December 13, 1837, Mackenzie and his followers established their headquarters on Navy Island, a sparsely populated settlement situated in Canadian territorial waters in the Niagara River.[49] Over the ensuing fortnight, the rebels' ranks swelled to almost

---

[46] Martin A, Rogoff & Edward Collins, Jr., *The Caroline Incident and the Development of International Law,* 16 BROOK. J. INT'L L 493, 494 (1990).
[47] *Id.*
[48] Thomas Nichols, *Address Delivered at Niagara Falls on the Anniversary of the Burning of the Caroline*, MERCURY & BUFFALONIAN EXTRA, Dec. 29, 1838 at 6-7.
[49] Rogoff & Collins, *supra* note 47, at 494.

one thousand men.[50] Almost immediately the rebels employed their increased strength to carry out harassing attacks on both the Canadian mainland and vulnerable British vessels steaming up the Niagara River.[51] Consequently, on December 23, 1837, Sir Francis Head, the Lieutenant Governor of Upper Canada, asked Henry Fox, the British Minister in Washington, to make a formal request that the United States government intervene to stop all pro rebel activity occurring on American soil.[52] Sir Head prodded Minister Fox to speak directly with the federal government because Head's earlier letter addressed to New York Governor William Marcy had gone unanswered.[53] For the purposes of this paper, these harassing attacks may be viewed as analogous to minor cyberattacks against the United States, during which our defenses are probed or code is embedded in out computer systems for future use. They are not major military operations, but they are nonetheless actions taken in contravention of the interests of the United States. An important fact in our analysis is that the "attacks" from the Caroline were clearly being launched from American soil, yet the United States government did nothing to stop them, even after such request was made by the Government of Canada. This construct will become very important as we consider attribution in the cyberattack context.

On December 29, 1837, impatient with the slow pace of diplomacy, Sir Head decided to act unilaterally to protect British interest and Canadian civilians from possible invasion and he summoned the Canadian militia and installed a cannon battery at Chippewa on the

---

[50] R. Y. Jennings, *The Caroline and McLeod Cases,* 32 AM. J. INT'L L. 82, 83 (1938). *See also* Rogoff & Collins, *supra* note 47, at 494.
[51] Jennings, *supra* note 51, at 83.
[52] Rogoff & Collins, *supra* note 47, at 494.
[53] *Id.*

Canadian mainland shore opposite Navy Island.[54] On that day as well, the *Caroline*, a privately owned American steamboat, made three trips to Navy Island conveying men and material to the rebel forces before being docked at Fort Schlosser, in New York State, directly across from Navy Island.[55] Despite the overwhelming evidence that the *Caroline* was ferrying arms and insurgents to Navy Island, there were nonetheless partisan contemporaries who vociferously denied the ship was anything but a civilian transport. As one writer declared in a passage representative of this viewpoint, the *Caroline* "was an American boat and . . . carrying an American flag. She was neither bought, nor chartered, nor hired by any party. . . . Why then should she fear – or wherefore should her crew be armed, or on watch to defend her?"[56]

The opinions of American pundits notwithstanding, upon observing that the *Caroline* was offloading "Stores of War" on Navy Island, Colonel Allan McNab, the commander of the Canadian militia, judged that the *Caroline*'s destruction would serve the double purpose of forestalling reinforcements and supplies from reaching the island as well as deprive the rebels of their means of access to the Canadian mainland.[57] Accordingly, later that night, Colonel McNab ordered Commander Andrew Drew of the Royal Navy to lead fifty-six Canadian militiamen in a clandestine mission to destroy the *Caroline*.[58] However, when Colonel McNab ordered the attack, he mistakenly believed that the *Caroline* was berthed in the British-Canadian territorial waters off Navy Island.[59] When

---

[54] *Id.*
[55] *Id.* at 494-95.
[56] Nichols, *supra* note 49 at 3.
[57] Jennings, *supra* note 51, at 83, 84.
[58] Doyle, *supra* note 45 at 11, 12.
[59] Id. at 12.

Commander Drew discovered the *Caroline* was not at Navy Island, he directed a portion of his men to float downstream in five boats where they found the *Caroline* docked at Fort Schlosser, New York.[60] Ignoring the fact that the ship was moored in American waters, Commander Drew ordered his men to board the vessel and "immediately commenced a warfare with muskets, swords, and cutlasses" upon the crew of the *Caroline*.[61] In the close quarters battle, two Americans were killed and the *Caroline* was "set on fire, cut loose from the dock, was towed into the current of the river, there abandoned, and soon after descended the Niagara falls."[62]

The intrusion of British-Canadian forces into sovereign United States territory and the destruction of the *Caroline* both served to inflame American anger.[63] Additionally, conflicting press reports about the incident spread confusion and fear, which lead to hardened perceptions on both sides of the border. As one American proto yellow journalist declared, the *Caroline* was engaged in harmless trade and was completely surprised by the "murderous attack . . . British officers and British soldiers sprang upon the deck, and mocking at the flag of our county and despising its boast of protection, commenced with insatiate greediness the work of death."[64] Initially, twelve crew members were reported missing and perhaps killed but later

---

[60] *Id.*
[61] Jennings, *supra* note 51, at 84.
[62] *Id.* at 84.
[63] James A. Green, *Docking the Caroline: Understanding the Relevance of the Formula in Contemporary Customary International Law Concerning Self Defense,* 14 CARDOZO J. INT'L & COMP. L. 429, 434 (2006). Indeed, even President Martin Van Buren who maintained a reputation for timidity denounced the incident as an "outrage." *Id.*
[64] Henry Brooke, *Book of Pirates,* 184 (1841).

investigation revealed that two people lost their lives: an African American sailor named Amos Durfee whose body was found on the quay with a musket ball through his head and a cabin boy known as "little Billy" who was shot while attempting to escape the militiamen.[65]

In addition to print media, woodcarvings and at least one dramatic contemporary painting by artist George Tattersall portrayed a sensational image of a burning yet intact *Caroline* hurtling toward the precipice of Niagara Falls amidst swift and powerful white capped waves.[66] The shocking image of a steamboat in conflagration plummeting over Niagara Falls captured the imagination of contemporaries to such an extent that even a decade later journalists dedicated to the truth needed to reiterate that "[i]t is impossible that the notorious Caroline steamer could have reached the great crescent in a state of integrity; these glorious rapids, which come onwards, leaping, roaring and exulting, like an army of hoary giants, must have torn the little craft to shreds as she passed through them."[67]

Although the actual death toll was made eventually made public, the melodramatic reporting drove a jingoistic impulse in both the United States and Canada. In the American press, "witnesses" told gripping tales that people near the river bank could hear the brave but doomed sailors' "wails . . . as they faced a double death" of burning and drowning.[68] Not to be outdone, Canadian patriots penned a "New Song" that lampooned the ironic history of the United States in which white slaveholding colonists decried their lack of

---

[65] Jennings, *supra* note 51, at 84. *See also McLeod's Trial,* THE NEW WORLD, Oct. 9, 1841, at 238.

[66] DEREK HAYES, CANADA: AN ILLUSTRATED HISTORY 129 (2004).

[67] *A Letter From the Falls of Niagara,* BAPTIST MEMORIAL & MONTHLY RECORD, Apr. 1, 1848, at 127.

[68] *Historical Narratives of Early Canada, available at: http://www.uppercanadahistory.ca/tt/tt6.html.*

freedom under the supposed yoke of British tyranny.[69] As the song boasted, when Mackenzie's rebel band was defeated in Ontario "[t]o Buffalo he did retreat and said We used him ill, Sir; The Buffalonians did sympathize And soon began to roar, Sir, They kicked up such a tarnation noise It reached the British shore Sir; . . . No slave shall ever breathe our air, No Lynch Law e'er shall bind us, So keep your Yankee mobs at Home, For Britons still you'll find us."[70]

Although tensions along the border remained elevated in the two years following the incident, diplomatic resolutions were muted.[71] During this period, diplomacy reached only so far as an exchange of letters between British Minister Henry Fox and United States Secretary of State John Forsyth.[72] While Secretary Forsyth demanded "redress" on behalf of the United States, Minister Fox insisted that the "piratical character of the steam boat *Caroline* and the necessity of self-defense and self-preservation, under which Her Majesty's subjects acted in destroying that vessel seem to be sufficiently established."[73] Additionally, Andrew Stevenson, the American Minister to Britain, sent a letter regarding the incident to Lord Palmerston, the British Foreign Secretary, where he argued that because there was no imminent danger to the Canadian militia, Britain could not claim to have acted in self-defense.[74] Much to

---

[69] *Id.*
[70] *Id.*
[71] Green, *supra* note 64 at 434.
[72] *Id.*
[73] *Id.*
[74] *Id.*

the ire of many Americans, Lord Palmerston took more than three years to respond to Stevenson's letter.[75]

Public furor in America over the destruction of the *Caroline* was reignited on November 12, 1840 with the arrest of a Canadian named Alexander McLeod. After McLeod bragged in a tavern of his involvement in the affair, he was arrested by American authorities and charged with both arson and the murder of *Caroline* crewmember Amos Durfee.[76] On December 13, 1840, Minister Fox wrote a letter to Secretary Forsyth denying that McLeod was involved in the incident and calling for his prompt release.[77] Minister Fox further argued that the attack on the *Caroline* was an incident of state action taken in self defense by persons under the authority of superior officers and therefore the United States could not proceed against persons in their individual capacity.[78] In reply, Secretary Forsyth dodged the substance of Fox's argument and merely explained that according to the American system of governance, the matter was within the jurisdiction of the New York trial court rather than the federal executive branch because McLeod was charged with an offense allegedly committed in New York and in violation of New York law.[79]

If Secretary Forsyth, an aged Southern Jacksonian Democrat, was not up to the task of a

---

[75] *Id.* In the interim period before Lord Palmerston answered Stevenson's letter, the American press railed against him as a "rash man, fond of a *coup d'etat*, willing to strike rashly . . . his course in regard to the Caroline steamer will not be forgotten. . . . [W]e may justly fear that he would prefer some sudden movement upon the United States to patient waiting for greater provocation." *Lord Palmerston*, NEW YORK SPECTATOR, Dec. 8, 1841, at 3.
[76] Rogoff & Collins, *supra* note 47, at 495.
[77] *Id.*
[78] *Id.* at 497.
[79] *Id.* at 495.

rigorous intellectual exchange with Minister Fox, his replacement Daniel Webster was a more than qualified opponent. A Phi Beta Kappa graduate of Dartmouth College, Webster was a constitutional lawyer who argued before the United States Supreme Court as well as a former Massachusetts Senator when he replaced Forsyth as Secretary of State on March 4, 1841.[80] Secretary Webster agreed with Minister Fox that McLeod should be released but Governor William Seward of New York, a staunch Whig, refused to issue a *nolle prosequi* to suspend further criminal proceedings.[81] Consequently, McLeod's case went forward until he was eventually acquitted at trial upon proof of an alibi.[82]

Although Secretary Webster's views regarding McLeod dovetailed with those of Minister Fox, he took strong exception to the prevailing British view that the destruction of the *Caroline* was justified as an act of self-defense.[83] In a letter to Minister Fox dated April 24, 1841, Secretary Webster set forth what became known as the *Caroline* doctrine.[84] In Secretary Webster's perspective, use of force by one state against another is permissible as an act of self-defense only if the force applied is both necessary and proportionate. Secretary Webster began his letter with an admonition that the Canadian militiamen's actions could not be justified "by any reasonable application or construction of the right of self defense under the laws of nations."[85] While

---

[80] IRVING H. BARTLETT, DANIEL WEBSTER 3 (1978).
[81] *Domestic Occurrences*, NEW HAMPSHIRE SENTINEL, Jan. 28 1841, at 308.
[82] *Id.*
[83] Rogoff & Collins, *supra* note 47, at 497.
[84] Jane Campbell Moriarty, *"While Dangers Gather": The Bush Preemption Doctrine, Battered Women, Imminence, and Anticipatory Self-Defense,* 30 N.Y.U. REV. L. & SOC. CHANGE 1, 7 (2005).
[85] Daniel Webster, *Case of the Caroline*, NILES' NATIONAL REGISTER, Sept. 24, 1842, at 57.

Secretary Webster admitted a nation's right to self-defense, he emphasized that the extent of this right must be judged on a case by case basis "and when its alleged exercise has led to the commission of hostile acts within the territory of a power at peace, nothing less than a clear and absolute necessity can afford ground of justification."[86] While acknowledging that the immensity of the border between the United States and Canada will likely lead to violence equally against the will of both governments, Secretary Webster underscored that regarding the *Caroline* incident, there was no reason to believe that American citizens committed hostile acts against Canadian interests.[87] After imparting this dubious remark, Secretary Webster then articulated the *Caroline* test whereby a government seeking to employ anticipatory self-defense must demonstrate "a necessity of self defense, instant, overwhelming, leaving no choice of means, and no moment for deliberation."[88] Adding a proportionality element, Secretary Webster went on to state that it will be for the British government to likewise show that "even supposing the necessity of the moment authorized them to enter the territories of the United States at all, [the militiamen] did nothing unreasonable or excessive; since the act justified by the necessity of self-defense, must be limited by that necessity, and kept clearly within it."[89]

The overwhelming majority of international law scholars consider Secretary Webster's *Caroline* test as the seminal definition of what constitutes permissible

---

[86] *Id.* Perhaps not surprisingly, Secretary Webster recalled the 18th century American prohibition against keeping standing armies in times of peace for the reason why the United States might have more trouble controlling its border population than Canada. *Id.*
[87] *Id.*
[88] *Id.*
[89] *Id.* at 58

use of force in anticipation of an attack on a state.[90] Indeed, as Professor Christine Gray remarked in 2000, the *Caroline* test has attained a mythical status not only for its definition of imminence but also for its requirement that the use of force be necessary and proportional to a coming attack.[91] Moreover, as described by British scholar R. Y. Jennings in his highly regarded 1938 article, the *Caroline* test had a humanist element because while it defined the right and left limits of national self-defense, it rescued the concept from "naturalist" notions of an absolute primordial right of self-preservation and thereby became the *locus classicus* of the law of self-defense.[92]

While scholars agree on the importance of the *Caroline* test in discussions of *jus ad bellum*, there is ongoing debate whether the doctrine is a suitable national security policy for the 21st century. In Dr. Michael W. Doyle's provocative recent book, he advanced the thesis that the *Caroline* test is woefully under-inclusive given the current threats to global security. In his view, Secretary Webster's doctrine merely justifies defensive reactions to imminent threats and such a parochial perspective could be disastrous in a thermonuclear age riven by terrorist acts and rogue nation states.[93]

Dr. Doyle opens his book by arguing that the *Caroline* incident is essentially ahistorical because it failed to meet the requirements of self-defense set forth by Secretary Webster and thus never represented the

---

[90] John Yoo, *Using Force,* 71 U. CHI. L. 729, 741 (2004).
[91] *Id. See also* CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 105 (2000).
[92] Jennings, *supra* note 14, at 192.
[93] Doyle, *supra* note 45, at 15. *See* Dodi-Lee Hect, *Tackling the Crisis of Anticipatory Defense: A First,* Second, *Third, and Fourth Strike at the Issue,* 47 COLUM. J. TRANSNAT'L L. 648, 648-49 (2009).

standards for which the case has become famous.[94] First, the attack on the *Caroline* was unnecessary because the British-Canadian militiamen enjoyed significant force superiority over the Mackenzie rebels on Navy Island. Second, the American government never intended to attack Canada. And third, there was no immediate threat to the British-Canadian forces.[95] Yet in Dr. Doyle's view, the real fault of the *Caroline* test lies not in its synthetic foundation but rather that the doctrine provides insufficient time for nations to guard their legitimate interests in self-defense when they still have some "choice of means" albeit no peaceful options and some "time to deliberate" among the dangerous choices left at their disposal. Accordingly, he insists that *Caroline* conditions are exceedingly rare in the real world and lists only the Netherlands' declaration of war on Japan as the one example of *Caroline* principles clearly validating an act of preemption.[96] Consequently, Dr. Doyle relegates the *Caroline* test to the status of an instructional cautionary tale that shows the difficulty of drawing a clear line separating imminent preemption from disallowed prevention.[97] The three factors mentioned by Dr. Doyle which he argues render the incident ahistorical are strikingly familiar to how a modern cyberattack may appear. First, the attack on the *Caroline* was unnecessary because the British-Canadian militiamen enjoyed significant force superiority over the Mackenzie rebels on Navy Island—this is almost always the case when one considers the United States as opposed to our enemies, with the possible exceptions of Russia and China. Second, the American government never intended to attack Canada- this goes directly to the

---

[94] Doyle, *supra* note 45, at 14.
[95] *Id.* at 13, 14.
[96] *Id.* at 15.
[97] *Id.* at 15, 16.

issue of attribution, an attack may easily be launched from a country, or routed through a particular country, which was not aware of, or intending for such attack to occur. And third, there was no immediate threat to the British-Canadian forces- this is also generally the case, however, in the realm of cyberattack, it is very difficult to judge what the action threat picture may be at any given moment.

Dr. Doyle further asserts that the potential for widespread carnage posed by weapons of mass destruction (WMDs) is heightened today as opposed to during the Cold War. In that period, the doctrine of mutual assured destruction imposed a nuclear stalemate because the Soviets were rationally deterrable while terrorist cells driven by religious fanaticism and martyrdom are far more difficult to deter.[98] For this reason, the demands of modern asymmetrical warfare necessitates that preventive responses that entail unilateral armed attack or multilateral enforcement measures remain lawful.[99] I would argue that the assertions of Dr. Doyle as related to concerns about WMDs are, at least conceptually, valid in the cyberattack arena, the ultimate in asymmetric warfare, as well.

If the *Caroline* case established the 19th century Anglo-American concept of national anticipatory self-defense, the United States reaffirmed its right ninety-one years later when it joined the Kellogg-Briand Pact.[100] Therefore, by the time the United States began negations to replace the League of Nations with a more dynamic international organization in the later stages of World

---

[98] *Id.* at 23, 24.
[99] *Id.* at 20.
[100] Amy E. Eckert & Manooher Mofidi, *Doctrine or Doctrinaire – The First Strike Doctrine and Preemptive Self-Defense Under International Law,* 12 TUL. J. INT'L & COMP. L. 117, 130 (2004).

War II, anticipatory self-defense was an accepted principle of international law.[101] As discussed above, pursuant to Article 51 of the United Nations (UN) Charter, "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense 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."[102]

Perhaps not surprisingly given the tenuous nature of global stability, Article 51 is the subject of continuing debate in the post 9/11 world. Unlike in the *Caroline* test, anticipatory self-defense is lawful under Article 51 only "if an armed attack occurs" and scholars are divided whether that phrase limits the right of self-defense such that it could properly be exercised by a victim state only in the wake of an attack.[103] Broadly speaking, the disputants of this question can be separated into two groups: the strict constructionists and the liberal constructionists.[104] The strict constructionists assert that Article 51 is constrained by a plain reading of the language and that the customary right to self-defense is safeguarded only in the situation of a prior armed attack.[105] Prominent strict constructionists such as Professor Ian Brownlie argue that if the UN Charter restrictions on the use of force were loosened, it would be impossible to determine whether a nation honestly resorted to their right of self-defense or merely invoked Article 51 to conceal their aggressive intentions toward

---

[101] *Id.*
[102] Keith A. Petty, *Criminalizing Force: Resolving the Threshold Question for the Crime of Aggression in the Context of Modern Conflict,* 33 SEATTLE U. L. REV. 105, 115 (2009).
[103] *Id.* at 137.
[104] *Id.*
[105] *Id.*

other states.[106] By contrast, the liberal constructionists posit that Article 51 should be construed in light of customary international law and that assuming the requirements of necessity, proportionality, and imminence are met, the right of self-defense allows the unilateral use of force in anticipation of an armed attack.[107] From this perspective, the Bush Doctrine was not the progenitor of the United States' preemption policy. Indeed, to take the most commonly cited example, President Kennedy's 1962 decision to forestall Soviet installation of short and intermediate ballistic missiles in Cuba by declaring a "quarantine" of the island stands as the most prominent example of American strategic preemption.[108]

Further complicating the debate between the strict and liberal constructionists is that the UN Charter procedures for regulating the use of force were never applied uniformly during the Cold War. First, due to their permanent seats on the Security Council, the United States and the Soviet Union could veto any effort to authorize force than ran counter to their national interests.[109] Second, warfare in the 20th century changed the calculus regarding the question of imminence because innovations in technology such as thermonuclear intercontinental ballistic missiles allowed an opponent to acquire a decisive advantage if allowed to strike first.[110] Third, the legitimate concern for humanitarian intervention defined as the use of force in the internal affairs of a nation to prevent large-scale deprivation of human rights imperils reading Articles 2

---

[106] Yoo, *supra* note 92, at 738-39.
[107] Eckert & Mofidi, *supra* note 102, at 137.
[108] David B. Rivkin, *The Virtues of Preemptive Deterrence*, 29 HARV. J. L. & PUB. POL'Y 85, 86 (2005).
[109] Yoo, *supra* note 92, at 742.
[110] *Id.* at 743.

(4) and 51 as anything but a prohibition on the use of force by states for any reason other than self-defense.[111]

As Dr. Doyle explains in *Striking First*, the Bush Doctrine emerged as a foil to both the *Caroline* test and Article 51 of the UN Charter. On September 12, 2002, President Bush addressed the UN and refocused international attention on the principles of preemptive self-defense and whether the United States should rely on this doctrine as a justification for the unilateral use of force.[112] As articulated, the Bush Doctrine was designed to prevent America's enemies from threatening the United States or its allies with WMDs.[113] Furthermore, the Bush Doctrine claimed the legal right to take military action to preempt gathering threats to United States national security with or without the sanction of the UN Security Council.[114] Additionally, President Bush asserted that the United States must remain proactive to prevent rogue nations that may harbor or assist terrorists from ever acquiring WMDs.[115] Consequently, a number of scholars believe that the Bush Doctrine re-cast anticipatory self-defense into an entitlement of preemption based on a different understanding of imminence where America "must adapt the concept of

---

[111] *Id.* For instance, the tragic case of Rwanda during the 1990s is but one example where a relatively minor intervention by the great powers might have prevented genocide. *Id.* at 744.

[112] Martinez, *supra* note 3, at 123.

[113] Tomasz Iwanek, *The 2003 Invasion of Iraq: How the System Failed,* 15 J. CONFLICT & SECURITY 89, 113 (2010).

[114] David B. Rivkin, et al., *Preemption and Law in the Twenty-First Century,* 5 CHI. J. INT'L L. 467, 467 (2005).

[115] Gregory E. Maggs, *How the United States Might Justify A Preemptive Strike On A Rogue Nation's Nuclear Weapon Development Facilities Under The U.N. Charter,* 57 SYRACUSE L. REV. 465, 469 (2007).

imminent threat to the capabilities of today's adversaries."[116]

To gain insight into the Bush Doctrine, certain legal scholars have turned to the past and examined the work of eminent 18th century international law theorist Emmerich de Vattel who perceived anticipatory self-defense as a fundamental legal right held by states and individuals alike.[117] Vattel's famous example is illustrative of the intellectual calculus behind the Bush Doctrine: "[o]n occasion, where it is impossible, or too dangerous to wait for absolute certainty, we may justly act on a reasonable presumption. If a stranger presents his piece at me in a wood, I am not yet certain that he intends to kill me; but shall I, in order to be convinced of his design, allow him to fire? What reasonable casuist will deny me the right of preventing him?"[118]

To be sure, Vattel's historical purpose was to justify military action against the French monarch but his exposition regarding preemptive self-defense is cited by Bush Doctrine supporters to illustrate their contention that preemptive self-defense is grounded in customary international law.[119] To further bolster their arguments, Bush Doctrine proponents look toward iconic World War II history. As the argument goes, Britain and France used their right to preemptive self defense to warn Nazi Germany that an invasion of Poland would be construed as a *casas belli*. At the time, Germany's military was not directly menacing either Britain or France especially in light of British Prime Minister

---

[116] Major John J. Merriam, *Natural Law and Self-Defense,* 206 MIL. L. REV. 43, 69 (2010).
[117] Rivkin, *supra* note 116, at 468.
[118] *Id.*
[119] *Id. See also* Michael J. Glennon, *Military Action against Terrorists under International Law: The Fog of Law, Self-Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter,* 25 HARV. J. L. & PUB. POL'Y 539, N. 62 (2002).

Neville Chamberlain's infamous pronouncement of "peace for our time" with Hitler and the only lawful means either nation had to issue its ultimatum to Germany was grounded in their right to anticipate future attacks.[120]

Yet scholars who take exception to the Bush Doctrine correctly point out that it obviates the Enlightenment notion of the rule of law that the state may generally employ harsh measures only on the basis of past wrongdoing that has been established to a high degree of certainty by a fundamentally fair process.[121] As Professor David Cole argues, the preventive paradigm rejects the rule of law's presumption against employing coercive force on the basis of conjecture regarding unpredictable future events.[122] Moreover, President Bush's concern that "[i]f we wait for threats to fully materialize, we will have waited too long" is a double-edged sword that can have disastrous consequences. In Professor Cole's view, while the preventive impulse may be salutary, it risks not only grievous errors but also erodes the respect that the rule of law offers to "regimes that play by the rules."[123] Furthermore, to the extent that the 2003 Iraq War is regarded as an act of preemptive self-defense, the difficult aftermath of that intervention may presage an era where nations resist resorting to large-scale preemptive self-defense. After all, the Iraq War highlighted the considerable policy difficulties that arise with unilateral preemptive action: an inability to attract allies, the dangers of faulty intelligence regarding a foreign state's weapons program and relations with

---

[120] Rivkin, *supra* note 116, at 470.
[121] DAVID COLE & JULES LOBEL, LESS SAFE, LESS FREE: WHY AMERICA IS LOSING THE WAR ON TERROR, 33 (2007).
[122] *Id.* at 34.
[123] *Id.*

terrorist groups, the political, economic, and human costs in pursuing elective wars, and the resistance level of radicalized factions to what is viewed by them as an unwarranted foreign invasion.[124]

In Dr. Doyle's perspective, the *Caroline* test is a relic of an age before WMDs while the Bush Doctrine is appallingly over-inclusive to the point where if it were adopted globally today "it could open the door to wars between Pakistan and India and perhaps even China and Taiwan."[125] Moreover, because the Bush Doctrine disregarded any pretense of an imminence requirement, it promulgated a subjective and open-ended standard that invites chaos because "every state will be preempting every other state's preventative strikes."[126] In his dissatisfaction with both the *Caroline* test and the Bush Doctrine, Dr. Doyle locates the UN and its Security Council in particular as the quintessential middle ground between two extremes. After all, reasons Dr. Doyle, pursuant to Article 39, the UN Security Council shall "determine the existence of *any* threat to the peace, breach of the peace or act of aggression" and take whatever action, including coercive embargoes and forcible measures by land, air, or sea, that the Security Council sees fit.[127] Acknowledging *realpolitik*, Dr. Doyle explains Article 39 contains two unresolved problems: first, the Security Council has failed to authorize force when it was arguably justified; and second, there is a dearth of adequate standards to guide the Security Council's deliberations.[128]

In his second essay, Dr. Doyle proposes a solution for the inherent lack of standards dilemma

---

[124] Sean Murphy, *The Doctrine of Preemptive Self-Defense*, 50 VILL. L. REV. 699, 747 (2005).
[125] *Id.* at 28. *See also* Hect, *supra* note 95, at 652.
[126] Doyle, *supra* note 45, at 26.
[127] *Id.* at 30 (emphasis in original).
[128] *Id.* at 33.

found in Article 39. Similar to the four pronged test espoused by Secretary Webster, Dr. Doyle argues the Security Council should be guided by the four elements of lethality, likelihood, legitimacy, and legality to gauge the seriousness of threats not yet imminent and the appropriate responses to them.[129] While three of the standards are perhaps conceptually straightforward, the legitimacy prong itself includes three elements: (1) weighing proportionately the threatened harm against the likely benefit-cost of the response; (2) limiting the response to the minimum necessary to effectively deal with the threat; and (3) seeking the relevant deliberation.[130] Applying these standards, Dr. Doyle argues that any nation considering anticipatory force should attain prior approval from the Security Council and that each voting member must state in public its reasons for accepting or rejecting the application to authorize prevention.[131] However, given the unpredictable record of the Security Council's decisions, if the vote is negative, individual nations could form a national commission to examine the facts before sending its report to the Security Council for an international investigation.[132] In the end, Dr. Doyle's expresses his remarkable if not altogether practical or convincing methodology in terms of a specific multiplicative equation where Justified Prevention = Lethality x Likelihood x Legitimacy x Legality.[133]

VI. APPLYING THE *CAROLINE* DOCTRINE TO CYBERATTACK IN THE 21ST CENTURY

Addressing a joint session of Congress on December 7, 1841 President John Tyler remarked on the

---

[129] *Id.* at 46.
[130] *Id.* at 57.
[131] *Id.* at 61.
[132] Doyle, *supra* note 45, at 62.
[133] *Id.* at 63.

Caroline incident and essentially repudiated what would become the Bush Doctrine. In the chaotic days following 9/11, Vice President Cheney espoused the "One Percent Doctrine" wherein if there is a one percent chance of a serious threat materializing, policymakers must perceive that threat as an event certain to occur.[134] Additionally, coupling Vice President Cheney's viewpoint with former Secretary of Defense Donald Rumsfeld's admission that "the absence of evidence is not evidence of absence" meant that a scintilla of evidence became a high probability and even situations where there is no evidence of even a one percent probability, that is not sufficient proof for the absence of sufficient provocation to warrant a preemptive attack with overwhelming force.[135] In direct contrast to the views expressed by members of the Bush Administration, President Tyler, calling upon her Majesty's government to apologize for burning the *Caroline*, steadfastly refused to sanction the right of any nation to engage in preemption action without sufficient provocation. In his understanding, to recognize preemption as "an admissible practice that each government . . . may take vengeance into its own hands . . . and in the absence of any pressing or overruling necessity, may invade the territory of the other, would inevitably lead to results equally deplored by both."[136]

In his comment on Dr. Doyle's essays, Dean Koh argues for a per se ban on unilateral anticipatory attack.[137] Dean Koh's position is admirable and humane and would that a world existed that a ban on anticipatory self-defense made the need for unilateral action obsolete.

---

[134] *Id.* at 107.
[135] *Id.*
[136] *President's Message to the Senate and House of Representatives of the United States,* ALEXANDRIA GAZETTE, Dec. 7, 1841, at 3.
[137] Doyle, *supra* note 45, at 107.

As it stands, Dean Koh is correct that Dr. Doyle's "Four Ls" of lethality, likelihood, legitimacy, and legality and their subparts is a complex test that would be difficult for bureaucracies to apply consistently.[138] On the other hand, there is a valid argument that Dean Koh is incorrect to take exception to the idea that in certain instances where the Security Council is paralyzed by indecision or political infighting, states have the discretion to take anticipatory unilateral action. The problem is that whereas Dean Koh is too hesitant to employ anticipatory self-defense, Dr. Doyle is both too eager to expand the parameters of the *Caroline* doctrine and overly reliant on the Security Council as an adequate response to the current challenges of WMDs, rogue states, and terrorism.

Despite the potential applicability of the *Caroline* test to the security exigencies of the 21st century, certain modifications are necessary to update Secretary Webster's test for an age in which cyberattacks can crisscross the world on the internet at the push of a button. The *Caroline* test distinguishes itself from the results of Bush Doctrine preemption measures because it curtails the right to national self-defense to situations where there is a real threat, the response is essential and proportional and all peaceful means of resolving the dispute were exhausted.[139] To be sure, Dean Koh's admonition regarding the difficulty of applying legal tests to real world instances is acknowledged but so too is the realization that it is likewise folly to make perfect the enemy of the good.[140]

---

[138] *Id.* at 101, 112.

[139] Amos N. Guiora, *Anticipatory Self-Defense and International Law – A Re-Evaluation,* 13 J. Conflict & Security L. 3, 8-9 (2008).

[140] Jide Nzelibe & John Yoo, *Rational War and Constitutional Design,* 115 YALE L. J. 2512, 2541 (2006)

Converting Secretary Webster's language into a modern legal test, an anticipatory strike must be (1) overwhelming in its necessity; (2) leaving no choice of means; (3) facing so imminent a threat that there is no moment for deliberation; and (4) proportional.[141] Consequently, a plain reading of the test implicates the liberal constructionist interpretation of Article 51 of the UN Charter that the right to self-defense entails a lawful use of force in anticipation of an armed attack. Therefore, given the current threats to global security, the "necessity" prong is the critical element of the *Caroline* tests that requires modernization. As Secretary Webster explained, the necessity prong is informed by the proportionality element because America "does not wish to disturb the tranquility of the world. . . . It is jealous of its rights . . . most especially, of the right of the absolute immunity of its territory, against aggression from abroad . . . while it will at the same time, as scrupulously, refrain from infringing on the rights of others."[142]

Recently, Professor Amos Guiora proposed using a "strict scrutiny" approach to self-defense against non-state actors wherein the executive would convince a court based on relevant, reliable, and corroborated intelligence that an anticipatory strike is appropriate.[143] Yet because the concept of employing a strict scrutiny standard for intelligence evaluation is fundamentally sound, the American government should extend it to include state actors as well. The logistics are perhaps less daunting than may first appear and involve two steps. First, the executive submits reliable intelligence information to a court of law. Second, the court examines the intelligence and subsequently rules as to

---

[141] Doyle, *supra* note 45, at 12, 13.
[142] Webster, *supra* note 87, at 58.
[143] See Guiora, *supra* note 142, at 16.

whether the information is sufficiently probative to warrant some form of anticipatory self-defense.[144] Importantly, this tribunal should be a creature of statute similar to the FISA court and thereby provide a means for the legislature to provide an additional check on both the executive and judicial branches. Moreover, unlike Professor Guiora's model, this proposal is not calling for an overwhelming change in the nature of the relationship between the executive and judicial branches because the executive would retain the power to veto the court's opinion or take direct action should for example an emergency situation involving WMDs occur.[145] This model, while solid in concept, is very problematic unless we are able to develop the appropriate means to attribute cyberattacks to particular actors. Or, in the alternative, are able to attribute the attacks to particular networks under within the territorial jurisdiction of nation states. If this becomes possible, with a high degree of accuracy, then we would be able to make reasonable requests that these nations restrict the activity going on within their borders. Given the fact that the internet is not generally restricted by territorial jurisdiction, we would have to greatly enhance cooperation between nations as well as fund international policing agencies such as Interpol.

Significantly, this model is not intended to be a perfect solution where if followed resulting history would show that the American government never undertook anticipatory self-defense action without sufficient provocation. A second acknowledged deficiency is that the model is specifically designed for the American system of governance and therefore cannot be transferred wholesale internationally. Nonetheless, because a single solution cannot solve every problem that is no reason to ignore the model's potential for

---

[144] *Id.* at 23, 24.
[145] *Id.* at 23.

positively influencing when and how the United States protects its citizenry. Instead, this schema is meant to safeguard the American government from reflexively taking potentially disastrous actions in the name of anticipatory self-defense. Essentially, this model provides a pressure valve designed to minimize the tragic results of mistaken intelligence or an unnecessary rush to armed conflict. In other words, the court would provide a moment of repose and deliberation where the executive could present its best arguments for the use of force and benefit from the insight contained in the court's opinion. In doing so, the court would act like an American Security Council without potentially sacrificing the safety of American citizens upon the interested decisions of the nations comprising the UN. As Dr. Doyle correctly states "in the world we live in today, where . . . the discretion of leaders is rightly suspect, we as citizens need to propose the standards that our leaders should employ when they claim to protect us."[146] Yet despite the laudable standards contained in Article 51, the UN is too haphazard a body to be given the ultimate responsibility of protecting Americans. In significant part, therefore, the answer to enhancing peace and security throughout the world lies within.

Looking ahead into the 21st century, it is likely that all manner of threats will continue, including cyberattack. As globalization, radicalism, and technological advances continue to change the means and nature of warfare, the United States requires bright-line rules regarding its use of anticipatory self-defense in the cyber context. Provided the current range of threats and uncertainties, it is unwise for America to look entirely to the interested UN to safeguard its citizenry. Similarly, given the disastrous consequences of preemption, the United States government should

---

[146] Doyle, *supra* note 45, at 159.

employ methods designed to assist the executive make reasoned and proportional responses. As modified by strict scrutiny analysis, the *Caroline* test is not expansive, obviates preemption but not anticipatory self-defense and is not overly reliant on the UN. Consequently, the updated *Caroline* doctrine may provide a flexible standard to meet the challenges of the coming decades provided the forensic ability to analyze the origin of attacks keeps pace with the technology allowing the attacks to occur.