"Cybervandalism" or "Digital Act of War?" America's Muddled Approach to Cyber Incidents Will Not Deter More Crises

Maj. Gen. Charles J. Dunlap, Jr., USAF (Ret.)†

I. Introduction

If experts say a "malicious [cyber] code"[1] has "similar effects"[2] to a "physical bomb,"[3] and that code actually causes "a stunning breach of global internet stability,"[4] is it really accurate to call that

---

† General Dunlap is a Professor of the Practice and the Executive Director of the Center on Law, Ethics and National Security at Duke University School of Law having retired from the Air Force's Judge Advocate General Corps in 2010 after more than 34 years of service. The author wishes to than Ms. Kathleen Cusack and Ms. Amy Richardson for their invaluable assistance with this article.

1 Joseph Menn et al., *Cyber Attacks Disrupt PayPal, Twitter, Other Sites*, REUTERS (Oct. 21, 2016, 9:31 PM), http://www.reuters.com/article/us-usa-cyber-idUSKCN12L1ME [https://perma.cc/XR8H-XQ3M].

2 Sara Ashley O'Brien, *'Unprecedented' Cyberattack Involved Tens of Millions of IP Addresses*, CNN (Oct. 22, 2016, 6:57 PM), http://money.cnn.com/2016/10/22/technology/dyn-cyberattack/ [https://perma.cc/RRY2-YDBB].

3 *Id.*

4 Menn et al., *supra* note 1.

event merely an instance of a "cyber attack"?[5]

Moreover, can you really expect to deter state and non-state actors from employing such code and similarly hostile cyber methodologies if all they think that they are risking is being labeled as a cyber-vandal subject only to law enforcement measures? Or might they act differently if it were made clear to them that such activity is considered an "armed attack"[6] against the United States and that they are in jeopardy of being on the receiving end of a forceful, law-of-war response by the most powerful military on the planet?[7]

Of course, if something really is just vandalism, the law enforcement paradigm, with its very limited response options, would suffice. But when malevolent cyber activity endangers the reliability of the internet in a world heavily dependent on a secure cyberspace, it is not merely vandalism. Rather, it is a national and international security threat that ought to be characterized and treated as such.[8] Unfortunately, the United States' current approach is too inscrutable and even contradictory to send an effective deterrence message to potential cyber actors. This needs to change.

This article proceeds in seven parts. Part II describes a recent breach of United States cyber security and the inherent vulnerability it reveals. Part III outlines the jumbled U.S. response to cyber-attacks and the current orientation of U.S. policy on the matter. Part IV argues that an ambiguous U.S. policy that leans toward a law enforcement approach rather than going through the law of war architecture is thwarting cyber deterrence. Even if

---

[5] Jilian Mincer, *Companies Urged to Use Multiple Vendors in Wake of Cyber Attack*, REUTERS (Oct. 23, 2016, 9:40 PM), http://www.reuters.com/article/us-usa-cyber-companies-idUSKCN12O041 [https://perma.cc/L6MH-GTZV].

[6] Collin Allan, *Was the Cyber Attack on a Dam in New York an Armed Attack?*, JUST SECURITY (Jan. 8, 2016, 1:10 PM), https://www.justsecurity.org/28720/cyber-attack-dam-armed-attack/ [https://perma.cc/4EWN-ZT36].

[7] *See* Jeremy Bender, *RANKED: The World's 20 Strongest Militaries*, BUS. INSIDER (Apr. 21, 2016, 10:24 AM), http://www.businessinsider.com/these-are-the-worlds-20-strongest-militaries-ranked-2016-4 [https://perma.cc/NL7X-ZU2L].

[8] *See* Cristina Dolan, *Cybersecurity Is A Global Threat To Democracy, Yet Not Well Understood*, FORBES TECH. COUNCIL (Nov. 7, 2016, 9:00 AM), https://www.forbes.com/sites/forbestechcouncil/2016/11/07/cybersecurity-is-a-global-threat-to-democracy-yet-not-well-understood/#5a5302375c2f [https://perma.cc/5UEM-T2PL].

recent cyber-attacks are not life threatening, the failure to establish an adequate proportionate response to these attacks will only incentivize further threats against U.S. national security [Part V]. Part VI explains how clarifying the law will ultimately enhance cyber deterrence. Finally, Part VII develops a broader view of the implications for Russia and China's mutual influence on cyber security law and the development of international norms. This article concludes with a thought to the future [Part VIII]. With each cyber-attack that passes without adequate response or proper characterization, the U.S. and others risk losing the global debate on cyber security and the role of International Humanitarian Law in deterring these forms of attack.

II. "A stunning breach of global internet stability."

Already it is evident that the United States has a cyber deterrence problem.[9] Consider the massive disruption of the Internet[10] that took place on October 21, 2016.[11] Twitter, PayPal, Spotify, and many other popular websites were virtually shut down when Dyn, a domain name system[12] ("DNS") provider that functions as a "switchboard" for an enormous amount of internet traffic, was shut down. Reuters characterized the cyber crisis as "a stunning breach of global internet stability."[13]

What made this cyber incident especially worrisome was that expert "attackers apparently used tens of thousands of hacked internet devices—household appliances such as digital video recorders, security cameras, and internet routers—to generate a massive amount of digital traffic" that jammed the system and grounded it to a halt several times.[14]

Although Web functionality was more or less reconstituted by the end of the day, the Dyn attack may signal things to come. A

---

9 *See generally* O'Brien, *supra* note 2 (discussing how a number of popular websites were inaccessible to some users "in a massive cyberattack with international reach").

10 *See id.*

11 *See* Menn et al., *supra* note 1.

12 *See id.*

13 *Id.*

14 Steven Melendez, *After Years Of Warnings, Internet Of Things Devices To Blame For Big Internet Attack*, FAST COMPANY (Oct. 23, 2016, 8:35 AM), https://www.fastcompany.com/3064904/after-years-of-warnings-internet-of-things-devices-to-blame-for-big-internet-attack [https://perma.cc/Z324-H3CZ].

retired intelligence officer ominously suggested that it may have been a probing attack—that is, one designated to enable an attacker to "eventually launch a devastating, Pearl Harbor-type cyber-attack."[15] Bruce Schneier commented that even before the most recent incident, the "precisely calibrated [cyber] attacks"[16] of recent months "feel[] like a nation's military cybercommand trying to calibrate its weaponry in the case of cyberwar."[17]

Nation-states are not alone in the quest to deter nefarious internet activity, as non-state actors can also cause serious disruption. For example, Mr. James Clapper, the Director of National Intelligence, indicates that "it 'appears to be preliminarily the case'" that a non-state actor may be responsible for the Dyn attacks.[18] Regardless, the vulnerability to a range of hostile actors is painfully evident: the devices exploited in this event, which are made with some parts "coming from Chinese suppliers [and] have weak or no password protections," are extremely common.[19] Intel Corporation predicts that the world will have 200 billion of such devices by 2020, so it is unlikely that we have seen the last of these cyber emergencies.[20]

III. Cyber Vandalism or Digital Acts of War?

Surveying the wide-ranging impact of the Dyn web calamity,

---

15 RC Porter, *Massive Cyber Attack on the Internet Underway; Is This a Probe? And, Part of a Larger Strategy by a Nation-State, Terrorists, Others – To Launch a Cyber Pearl Harbor-Type Attack?*, FORTUNA'S CORNER (Oct. 21, 2016), http://fortunascorner.com/2016/10/21/massive-cyber-attack-on-the-internet-underway-is-this-a-probe-and-part-of-a-larger-strategy-by-a-nation-state-terrorists-others-to-launch-a-cyber-pearl-harbor-type-attack/ [https://perma.cc/P8DU-SMBR] [hereinafter *Massive Cyber Attack*].

16 Bruce Schneier, *Someone Is Learning How to Take Down the Internet*, SCHNEIER ON SECURITY (Sept. 13, 2016), https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html [https://perma.cc/D5EB-PLYY].

17 *Id.*

18 Laura Wagner, *U.S. Intelligence Chief Says Internet Outage Was Likely the Work of a Non-State Actor*, SLATE (Oct. 26, 2016, 12:00 PM), http://www.slate.com/blogs/future_tense/2016/10/26/james_clapper_says_internet_outage_was_likely_the_work_of_a_non_state_actor.html [https://perma.cc/Y5DH-9V93].

19 David Sanger & Nicole Perlroth, *A New Era of Internet Attacks Powered by Everyday Devices*, N.Y. TIMES (Oct. 22, 2016), https://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html?_r=0 [https://perma.cc/9R6C-7P3Z].

20 *See id.*

an analyst observed that "[e]ven though [the malware involved in the attack is] not a physical bomb, it has some similar effects."[21] The question then is—does the United States consider this unprecedentedly severe incident, involving as it does a cyber capability that has similar effects to a physical bomb, to be a digital act of war?

Evidently not. Even though the facts of the massive shutdown would seem to equate the incident with a traditional kinetic attack, NBC news reports a senior U.S. intelligence official as rather dismissively classifying the incident as just "a classic case of internet vandalism."[22]

The official's characterization conforms to what the United States has said previously about the legal status of certain cyber events. It is important to understand that "act of war" is a political term, not one of international law. In the post-UN Charter era, the "act of war" idiom is at odds with the underlying thrust of the Charter and especially Article 2(4).[23] Article 2(4) demands that "[a]ll members shall refrain in their international relations from the threat 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."[24] In essence, "war" as it is historically understood, is all but illegal; disputes are to be resolved by peaceful means.

There are, however, narrow exceptions to the prohibitions against the use of force. Force is allowed when the Security Council authorizes it under Article 42 of the Charter.[25] Additionally, a nation may employ force in self-defense when it has suffered what Article 51 describes as an "armed attack."[26]

---

21 O'Brien, *supra* note 2.

22 Berkeley Lovelace, *Dyn Says Cyberattack "Resolved" After Services Shut Down*, NBC NEWS (Oct. 21, 2016), http://www.nbcnews.com/tech/tech-news/dyn-says-cyberattack-resolved-after-services-shut-down-n670926 [https://perma.cc/EJ2R-NFB2].

23 U.N. Charter art. 2, ¶4.

24 *Id.*

25 *Id.* art. 42.

26 *Id.* art. 51 ("Nothing 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. Measures taken by Members in the exercise of this right of self-defense 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

The law does not define exactly what form of forceful response a country may take in a legitimate act of self-defense except to say it must be necessary and proportional.[27] Nor does it limit a self-defense response in a cyber-situation to an "in-kind" response.[28] The United States, for example, could initiate a self-defense response to a cyber-attack which might include the use of traditional kinetic force involving conventional military weapons.[29]

The language of the United States' response to the Dyn attack renders unclear as to when the United States considers itself to have suffered an "armed attack" in the cyber context, so as to trigger a right to self-defense under Article 51. Despite the enormous dimensions of the Dyn onslaught, the official's claim that it is simply "cyber vandalism" (as opposed to any sort of "attack") seems to suggest that the U.S. doesn't consider it serious enough to permit a self-defense response within the meaning of Charter. This characterization is rather ironic as the United States has previously expressed a rather aggressive stance regarding what sort of cyber incidents could authorize forceful acts in self-defense.

In a seminal 2012 speech, the then-Legal Advisor to the State Department Harold Koh staked out the U.S. position.[30] Initially, he affirmed that the "established jus ad bellum rules do apply to uses of force in cyberspace."[31] He went on to explain that "cyber

---

present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."). Most nations also believe Article 51 incorporates an inherent right to act in anticipatory self-defense when an armed attack against them is imminent.

27 U.N. Charter arts. 42, 51.

28 *Id.*

29 *See* Graham Allison, *How the US and China Will Go To War*, NATIONAL INTEREST (Apr. 12, 2017), http://nationalinterest.org/feature/how-america-china-could-stumble-war-20150?page=7 [https://perma.cc/J2MK-ZRZ9] (explaining that a country, in this instance China, could use kinetic weapons as a result on a mainland attack).

30 Ellen Nakashima, *Cyber Attacks Could Trigger Self-Defense Rule, U.S. Official Says*, WASH. POST (Sept. 18, 2012), https://www.washingtonpost.com/world/national-security/us-official-says-cyberattacks-can-trigger-self-defense-rule/2012/09/18/c2246c1a-0202-11e2-b260-32f4a8db9b7e_story.html?utm_term=.2f59aab3e7be [https://perma.cc/JF45-35A5].

31 Chris Borgen, *Harold Koh On International Law in Cyberspace*, OPINIO JURIS (Sept. 19, 2012), http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/ [https://perma.cc/2BD4-QXQ3]; Karma Nabulsi, *Jus Ad Bellum/ Jus In Bello*, CRIMES OF WAR, http://www.crimesofwar.org/a-z-guide/jus-ad-bellum-jus-in-bello/ [https://perma.cc/B3WU-82AL] (Jus ad bellum is that "branch of law that defines

activities that proximately result in death, injury, or significant [physical] destruction would likely be viewed as a use of force."[32]

Pointedly, he also said that "if the physical consequences of a cyber-attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber-attack should equally be considered a use of force."[33] In light of the claim that last week's incident has "some similar effects" to a "physical bomb," was the Koh threshold met? Or does the absence of "death, injury, or significant destruction" make it fall short in the U.S.'s view?[34]

It is not clear. Koh makes it hard to determine because he said that the U.S. "has for a long time taken the position that the inherent right of self-defense potentially applies against any illegal use of force" adding that "[in the U.S.'s] view, there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response."[35] In other words, from the U.S. perspective, there is no difference between "force" as used in Article 2 of the UN Charter and "armed attack" as used in Article 51.[36]

This interpretation of the law is, internationally, a distinctly minority view, as Professor Michael Schmitt and other cyberlaw experts have noted.[37] It creates a complication because most interpretations of international law find that there are actions which might constitute "force" under Article 2, but not involve the kind of proximate "death, injury, or significant destruction" typically associated with an "armed attack."[38] Citing *Nicaragua v. U.S.*, Schmitt provides an illustration with obvious implications for the U.S. position on cyber uses of force:

> [T]he International Court of Justice held that although merely funding guerrillas who were conducting hostilities against

---

the legitimate reasons a state may engage in war and focuses on certain criteria that render a war just.").

32 Borgen, *supra* note 31.

33 *Id.*

34 O'Brien, *supra* note 2.

35 Borgen, *supra* note 31.

36 *See* Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and The Cyber "Use-Of-Force" Debate*, 67 JFQ 40, 41–42 (2012).

37 *Id.*

38 *See* Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. 13, 19 (2012).

> another State did not reach the use of force threshold, arming and training them did. The holding suggests that an act need not have immediate physical consequences to comprise a use of force.[39]

When the Nicaragua holding is juxtaposed with Koh's assertion that "force" and "armed attack" are conterminous, it seems that the United States should consider a grave cyber event like the Dyn attack as the legal equivalent to an "armed attack" even if it did not produce "death, injury, or significant destruction."[40] After all, if the U.S. position is that any use of force is enough to justify an Article 51 response, disrupting half the global internet with a methodology with effects similar to a "physical bomb" would certainly seem to be at least as significant as arming and training guerrillas in a single country.

To consider an incident as severe as the Dyn case as sufficient to put the perpetrators at risk of a forceful self-defense response not only would conform to the existing U.S. interpretation, but also could signal a norm evolution consonant with Article 51. The 2013 Tallinn Manual, which many consider to be the leading treatise on the international law applicable to cyberwar, does find that "force" as used in Article 2(4) is different from the arguably more egregious "armed attack" as set out in Article 51.[41] At the same time, however, its included commentary reports that the group of experts who drafted the Tallinn Manual found the law was "unsettled" as to whether "actions that do not result in injury, death, damage or destruction, but which otherwise have extensive negative effects" could amount to an armed attack.[42]

In fact, we may be seeing a shift towards broader acceptance of the idea that cyber incidents with widespread adverse effects are enough to trigger an Article 51 response, even without any physical injuries or damage. In 2015, two years after the issuance of the Tallinn Manual, Professor Schmitt, who was the project's director, agreed that if a cyber operation shut down the national

---

39 *Id.* at 20; Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Summary of the Summary of the Judgment, 1986 I.C.J. Rep. 14 (June 27), http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5 [https://perma.cc/UB4L-XVDW].

40 *See* Schmitt, *supra* note 38.

41 MICHAEL N. SCHMITT ET AL., TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 42 (2013).

42 *Id.* at 56.

economy without death or destruction, it would nevertheless "probably" meet the more demanding "armed attack" threshold.[43]

In addition, UCLA's Professor Kristen Eichensehr noted the conundrum that "cyber weapons create the possibility of actions that cause severe harm to the victim, but nevertheless do not result in physical damage or injury to persons."[44] Consequently, she predicted, "it is possible that over time a cyber-specific definition of armed attack may arise that does not require physical harm, even though physical harm is required for armed attacks caused by other sorts of weapons."[45] With the experience of the Dyn case, that time may be now.

The U.S. interpretation of the law would seem to be open to such a finding. In the first place, the 2015 U.S. Department of Defense's ("DoD") Law of War Manual ("Manual") confirms in Chapter XVI ("Cyber Operations") that the law of war applies to cyber, but admits that "[p]recisely how the law of war applies to cyber operations is not well-settled, and aspects of the law in this area are likely to continue to develop, especially as new cyber capabilities are developed and States determine their views in response to such development."[46]

Next, the Manual goes on to essentially incorporate the Koh approach by saying, "if cyber operations cause effects that, if caused by traditional physical means, would be regarded as a use of force under *jus ad bellum*, then such cyber operations would likely also be regarded as a use of force."[47] This intriguingly suggests that a use of force sufficient for jus ad bellum might exist even in the absence of physical injuries or destruction.

How? In listing examples of acts that could meet the use of force standard, the Manual says: "cyber operations that cripple a military's logistics systems, and thus its ability to conduct and sustain military operations, might also be considered a use of force

---

43 Ryan Fairchild, ***When Can a Hacker Start a War?***, PACIFIC STANDARD (Feb. 6, 2015), https://psmag.com/when-can-a-hacker-start-a-war-9a59bfcf9526#.ktt4xu55p [https://perma.cc/A6FH-HDAR].

44 Kristen E. Eichensehr, *Cyberwar & International Law Step Zero*, 50 TEX. INT'L L.J. 355, 374 (2015).

45 *Id.*

46 OFFICE OF GEN. COUNSEL, DEP'T. OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL 994 (June 2015) [hereinafter DOD LAW OF WAR MANUAL].

47 *Id.* at 998.

under *jus ad bellum*."[48] The footnote supporting this proposition points to a 1999 publication, *An Assessment of International Legal Issues in Information Operations*, by the DoD Office of the General Counsel.[49] That document says:

> Even if the systems attacked were unclassified military logistics systems, an attack on such systems might seriously threaten a nation's security. For example, corrupting the data in a nation's computerized systems for managing its military fuel, spare parts, transportation, troop mobilization, or medical supplies may seriously interfere with its ability to conduct military operations. In short, the consequences are likely to be more important than the means used.[50]

This illustrates that at least from the DoD's perspective, if a cyber event has significant a *casus belli* even in the absence of physical injuries or destruction. The relevant question then would be: doesn't an assault that caused "a stunning breach of global internet stability" and shut down half the internet qualify?

Complicating the issue is the July 2016 testimony before Congress by the State Department's Coordinator for Cyber Issues, Christopher Painter as to what he called "digital acts of war."[51] According to Painter, in determining on a "case-by-case, fact-specific" basis whether a cyber activity constitutes an "armed attack" "sufficient to trigger . . . [the] right of self-defense," "the actual or anticipated effects of a particular incident" are of "primary importance."[52] Painter says "the U.S. government believes that states should consider the nature and extent of injury or death to persons and the destruction of, or damage to, property."[53] If the cyber act "proximately" causes "death, injury,

---

48 *Id.* at 998–99.

49 *Id.* at 999 n.21.

50 *Id.* (quoting in an explanatory parenthetical the OFFICE OF GEN. COUNSEL, DEP'T. OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (2nd ed., 1999), reprinted in 76 U.S. NAVAL WAR COLLEGE INT'L L. STUDIES 459, 483 (2002)).

51 *See Digital Acts of War: Evolving the Cybersecurity Conversation: Hearing on "Digital Acts of War: Evolving the Cybersecurity Conversation" Before the H. Comm. on Oversight and Government Reform Subcommittees on Information Security and National Security,* 114th Cong. 4 (2016) (testimony of Christopher M. E. Painter, Coordinator for Cyber Issues, U.S. Department of State).

52 *Id.*

53 *Id.*

or significant destruction" it "likely would be viewed as an armed attack."[54]

The problem, of course, is that while Painter's formulation includes the obvious "death, injury, or significant destruction" standard,[55] it does not necessarily preclude finding that non-destructive cyber events could also produce "actual or anticipated effects"[56] sufficient to permit an Article 51 response. It seems that Painter intentionally meant to be rather enigmatic as he also claims:

> As a general matter, states have not sought to define precisely (or state conclusively) what situations would constitute armed attacks in other domains, and there is no reason cyberspace should be different. In fact, there is a good reason not to articulate a bright line, as strategic ambiguity could very well deter most states from getting close to it.

IV. Does Calling a Severe Disruption "Cyber Vandalism" Deter or Incentivize?

While there may be a place for ambiguity in strategic deterrence, the Dyn cyberattack of late 2016 shows that it is not working for the United States. The reason for this could well be the trivializing public characterization the government has been giving to events like the Dyn incident, in addition to the government's tendency to apply similar language even when physical damage actually results. In the law, words do matter. Portraying something as "cyber vandalism" would not permit the United States to legally respond in the same way it could if it had been struck by a "physical bomb." This discrepancy in incident description could have serious consequences for the development of deterrence in relation to cyber events.

Put another way, vandalism is ordinarily understood as a minor criminal law matter involving judicial processes, and not something that would sanction the use of force. As an international law matter, retorsion[57] and countermeasures[58] might

---

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *What is Retorsion*, BLACK'S LAW DICTIONARY (2d ed. 1910), http://thelawdictionary.org/retorsion/ [https://perma.cc/HLF8-UASL].

[58] Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The*

be available as responses to vandalism—as may other remedies under the law of state responsibility[59]—but none of these options allow the use of force. By contrast, activities that equate to "physical bombs" could readily be viewed as a national security threat sufficient to prompt a pre-emptive response, where an acceptable response could be the necessary and proportional use of force to counter them.[60] To reiterate, the law enforcement paradigm suggested by "vandalism" is very different from the law of war architecture that arises from national security threats, as the "law enforcement" response to vandalism is much more limited.[61]

Yet even where the cyber incident unquestionably fulfills the "physical damage" criteria, the United States inexplicably softens its classification. For example, in 2014, President Obama used the term "cybervandalism" in denying that North Korea's cyber operation against Sony Pictures constituted an "act of war."[62] However, the Department of Defense Cyber Strategy document released in April of 2015[63] described the Sony incident in much more serious terms, saying:

> North Korea conducted a cyberattack against Sony Pictures Entertainment, *rendering thousands of Sony computers inoperable* and breaching Sony's confidential business information. In addition to the *destructive* nature of the *attacks*, North Korea stole digital copies of a number of unreleased movies, as well as thousands of documents containing sensitive data regarding celebrities, Sony employees, and Sony's business

---

Countermeasures Response Option and International Law, 54 VA. INT'L L.J. 697, 700–01 (2014) (defining countermeasures).

59 *See* G.A. Res. 56/83, 223–25 (Dec. 12, 2001) (describing remedies available in different courts based on the law of state responsibility).

60 *See* RYAN DOWDY ET AL., LAW OF ARMED CONFLICT DESKBOOK 38 (5th ed. 2015) (reaffirming the use of preemptive force against rogue states that present a threat to the United States).

61 *See* Jan Hessbruegge, *The Right to Life as the Jus ad Bellum of Non-International Armed Conflict (A Reply to Lieblich)*, JUST SECURITY (OCT. 27, 2016, 1:48 PM), https://www.justsecurity.org/33906/life-jus-ad-bellum-non-international-armed-conflict-a-reply-lieblich/ [https://perma.cc/RUA7-WJ6E] (stating "[u]nder international law, the human right to life tightly limits the use of lethal force to contain threats to law and order").

62 Eric Bradner, *Obama: North Korea's Hack Not War, But 'Cybervandilism'*, CNN (Dec. 24, 2014), http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism/ [https://perma.cc/V4Z6-LJGU].

63 U.S. DEP'T OF DEF., THE DOD CYBER STRATEGY (2015).

> operations. North Korea accompanied their cyberattacks with *coercion, intimidation, and the threat of terrorism*. The North Korean attack on Sony was one of the most destructive cyberattacks on a U.S. entity to date.[64]

Likewise, Assistant to the President for Homeland Security and Counterterrorism, Lisa Monaco, said in July of 2016 that the Sony attack "had crossed a threshold," adding that it "was both destructive, it fried the computers of Sony Pictures, took them offline[,] and it was coercive."[65] Given the evidence of physical destruction, it is hard to argue that the Sonny attack did not meet the United States' —and indeed the world's— definition of "armed attack.".

Regarding last summer's hack of thousands of Democratic National Committee ("DNC") emails, Ms. Monaco emphasized the gravity of the event, calling it a "serious, serious issue, a serious thing if there is deliberate intrusion for the purpose of coercing and influencing the political process."[66] The distinctive nature of the target—the U.S. election system—caused John Brennan, Director of the Central Intelligence Agency, to conclude that "[o]bviously interference in the U.S. election process is a very, very serious matter."[67]

Despite the consensus about the seriousness and uniqueness of cyber efforts to interfere with the political process, the President again sought to downplay the incidents. In early September, he "acknowledged that the Russians have been attacking U.S. institutions on the internet"[68] but has also said that:

---

64 *Id.* at 2 (emphasis added).

65 THE ASPEN INST., ASPEN SECURITY FORUM 2016: THE VIEW FROM THE WEST WING 13 (2016), http://aspensecurityforum.org/wp-content/uploads/2016/07/lisa-monaco-the-view-from-the-west-wing.pdf [https://perma.cc/2QXX-MMVB].

66 *Id.* at 17; *see also* Aaron Blake, *Here are the Latest, Most Damaging Thing in the DNC's Leaked Emails*, FIX (July 25, 2016), https://www.washingtonpost.com/news/the-fix/wp/2016/07/24/here-are-the-latest-most-damaging-things-in-the-dncs-leaked-emails/?utm_term=.9c955ec7c00d [https://perma.cc/C2WR-DR7S] (regarding the DNC hack).

67 THE ASPEN INST., ASPEN SECURITY FORUM 2016: A CANDID CONVERSATION WITH THE DIRECTOR OF THE CIA 29 (2016), http://aspensecurityforum.org/wp-content/uploads/2016/07/a-candid-conversation-with-the-director-of-the-cia.pdf [https://perma.cc/XU94-KEYY].

68 Dave Boyer, *Obama Says He Doesn't Want 'Wild West' Cyberwar with Russia*, WASH. TIMES (Sep. 5, 2016), http://www.washingtontimes.com/news/2016/sep/5/obama-says-he-doesnt-want-wild-west-cyberwar-russi/ [https://perma.cc/UT43-XRRG].

> Our goal is not to suddenly in the cyber arena duplicate a cycle of escalation that we saw when it comes to other arms races in the past, but rather to start instituting some norms so that everybody's acting responsibly . . . . What we cannot do is have a situation in which suddenly this becomes the wild, wild West, where countries that have significant cybercapacity start engaging in unhealthy competition or conflict through these means.[69]

By early October, the U.S. government was nevertheless explicitly accusing the Russian government of directing what the U.S. government was calling "compromises" of—but not "attacks" on—cyber systems.[70] The U.S. government claimed that "thefts and disclosures" were "intended to interfere with the [U.S.] election process."[71] Without referencing a legal basis, Josh Ernest, the White House Press Secretary, said in October 2016—before the Dyn case—that there would be no legal response to these "thefts and disclosures."[72] Ernest therefore added to the legal muddle because, although there was no legal response, he insisted that there would be a "proportional" response.[73]

The response to a criminal matter like a "compromise" or "disclosure" or even a "theft" is a judicial one; a "proportional" response is, however, the language of force sounding in *jus ad bellum*, not law enforcement. Confusingly, he also said it "is unlikely that our response would be announced in advance"[74]—again, *jus ad bellum* terms mixed with criminal law rhetoric. It is true, that an "armed attack" could also be a criminal offense, but the way it is being publicly presented suggests little cognizance of the critical differences between the two legal regimes, or the effect

---

69 *Id.*

70 Press Release, Department of Homeland Security, Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security (Oct. 7, 2016), https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national [https://perma.cc/3SVK-CTNP].

71 *Id.*

72 Josh Ernest, Press Sec'y, The White House, Press Gaggle by Press Sec'y Josh Ernest en route to Greensboro, NC (Oct. 11, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/10/11/press-gaggle-press-secretary-josh-earnest-en-route-greensboro-nc [https://perma.cc/Y5ZM-DVYU] [hereinafter Ernest Press].

73 *Id.*

74 *Id.*

on deterrence those differences might have.

V. Deterrence and Dithering?

Mr. Ernest further complicated the matter when he asserted "[i]t's certainly possible that the President could choose response options that we never announce."[75] This is hardly what would or should occur if the actions were really just vandalism—a criminal law matter—and is not the way to go about deterring actors from similar behavior. How will people be deterred if the consequences are unknown? Adding to the confusion are press reports that suggest experts are not optimistic about the United State's vision of what the "proportional" response should be; announced or not.

Harvard Law Professor Jack Goldsmith,[76] long a critic of what he calls the United State's "feckless" cyber deterrence policy,[77] warned that the U.S. government's "dithering"[78] in response to previous cyber incidents (including the 2015 Office of Personnel Management data breach[79] that may have affected as many as 22 million people[80]) was dangerous. Professor Goldsmith avowed that:

> Such a pattern of vacillation in response to very damaging cyber-operations will not deter our adversaries; it will embolden them. It will especially embolden them since the responses the USG finally settles on are much less than proportionate to the

---

[75] *Id.*

[76] Jack Landman Goldsmith is the Henry L. Shattuck Professor of Law at Harvard University. Professor Goldsmith previously served in the Justice Department and Department of Defense during the George W. Bush Administration. http://hls.harvard.edu/faculty/directory/10320/Goldsmith [https://perma.cc/LA3F-W44S].

[77] Jack Goldsmith, *The United States' Feckless Cyber Deterrence Policy*, LAWFARE (Aug. 1, 2015), https://www.lawfareblog.com/united-states-feckless-cyber-deterrence-policy [https://perma.cc/7UWV-XGYD].

[78] Jack Goldsmith, *The DNC Hack and (the Lack of) Deterrence*, LAWFARE (Oct. 9, 2016), https://www.lawfareblog.com/dnc-hack-and-lack-deterrence [https://perma.cc/M54B-YQDL].

[79] *Cybersecurity Resource Center*, OPM.GOV, https://www.opm.gov/cybersecurity/cybersecurity-incidents/ [https://perma.cc/6D8X-Y288].

[80] David Perera, *Chaffetz: OPM Data Breaches May Affect 32 Million*, POLITICO (June 24, 2015), http://www.politico.com/story/2015/06/opm-data-breach-jason-chaffetz-119374 [https://perma.cc/J4TT-2H59] (explaining that 22 million was the figure issued by the OPM).

damage caused.[81]

Susan Hennessy, a legal scholar at the Brookings Institute, differed somewhat with Goldsmith and instead asserted that U.S. deterrence policy has been successful to the extent that the United States "has never been the victim of a cyber-attack that genuinely threatened lives."[82] She also helpfully notes that the "[Obama] Administration quietly released its policy on cyber deterrence late last year."[83] The policy stated: "the Administration is most concerned about threats that could cause wide-scale disruption, destruction, loss of life, and significant economic consequences for the United States and its interests."[84] Such attacks would include (but are not limited to):

- Cyber-attacks or other malicious cyber activity intended to cause casualties;[85]
- Cyber-attacks or other malicious cyber activity intended to cause significant disruption to the normal functioning of U.S. society or government, including attacks against critical infrastructure that could damage systems used to provide key services to the public or the government;[86]
- Cyber-attacks or other malicious cyber activity that threatens the command and control of U.S. military forces, the freedom of maneuver of U.S. military forces, or the infrastructure on which the U.S. military relies to defend U.S. interests and commitments;[87]
- Malicious cyber activity that undermines national economic security through cyber-enabled economic espionage or sabotage.[88]

Hennessey believes that tampering with the mechanisms of the election is still a "below the threshold" activity (that is, below the "armed attack" standard), although she agrees that such actions

---

81 Goldsmith, *supra* note 78.

82 Susan Hennessey, *Is US Deterrence Strategy More than (Russian) Roulette?*, LAWFARE (Oct. 12, 2016, 1:16 PM), https://www.lawfareblog.com/us-cyber-deterrence-strategy-more-russian-roulette [https://perma.cc/J6ED-9363].

83 *Id.*

84 *Id.*

85 *Id.*

86 *Id.*

87 *Id.*

88 Hennessey, *supra* note 82.

combined with others might collectively exceed it.[89] She also points to Phil Walters' work,[90] describing a sophisticated Russian strategy to employ various "below established threshold activities" ("BETA"), and its relation to deterrence.[91] Ms. Hennessey argues that while the United States' deterrence is working, in that it is "effectively preventing very serious activity, at least for now," its responses to BETA," are reactive and unpredictable, which undercuts the deterrent effect."[92] She closes by articulating a belief that:

> U.S. deterrence policy currently has the feeling of roulette. Maybe the house still wins overall, but it is clear that actors like Russia are happy to keep spinning the wheel while they're ahead.[93]

Less than two weeks after Hennessey wrote her piece, an undeterred actor launched the Dyn assault that hobbled half of the Web.[94] Even the Department of Homeland Security admitted just a month before the Dyn attack that the U.S. "has experienced increasingly severe and significant cyber incidents affecting both the private sector and Federal Government."[95] That admission, along with the new Dyn case, ought to make it clear that the United States needs to retool its cyber deterrence strategy.

VI. What to Do?

Clarifying the law on cyber security and the rights of countries to self-defense against cyber-attacks will help to alleviate these struggles with ambiguity.

---

89 *Id.*

90 Phil Walter, *National Security Adaptations to Below Established Threshold Activities*, LAWFARE (Aug. 15, 2016, 8:37 AM), https://www.lawfareblog.com/national-security-adaptations-below-established-threshold-activities [https://perma.cc/3ZZA-BTNG].

91 *Id.* (discussing Russian use of hybrid warfare to avoid the checks imposed upon them by U.S. and NATO nuclear deterrents).

92 Hennessey, *supra* note 82.

93 *Id.*

94 Andy Ozment, *National Cyber Incident Response Plan Now Available for Public Comment*, DEP'T HOMELAND SECURITY (Sep. 30, 2016), https://www.dhs.gov/blog/2016/09/30/national-cyber-incident-response-plan-now-available-public-comment [https://perma.cc/HHN8-GFRT].

95 *Id.*

A. Clarifying Terms

Deterrence is a devilishly complex endeavor, especially where cyber is concerned - but clarifying the law can help. Shortly after the Dyn incident, Mr. Clapper lamented:

> [W]e don't have enough body of law yet. We haven't, in my opinion — this is not company policy; it's just me speaking — but we have not been able to generate either the substance or the psychology of deterrence in the cyber realm. And that's going to continue to be an issue for us.[96]

Regardless of whether Clapper is actually correct about whether an adequate body of law exists to support deterrence, it is true that many others have that perception.[97] In truth, the law itself may not be as much as of a problem as the proper application of the law (and especially the United States' view of it) to the facts. That proper application can be facilitated by cleaning up the language officials use in regards to cyber incidents, and to synchronize it with announced U.S. interpretations.

To effectively deter, consistency and accuracy of language is indispensable. Since the United States has elected to characterize any use of force as sufficient to trigger a right to self- defense under Article 51, when events occur that plainly meet that standard (and even in the event that they cross the more demanding "armed attack" threshold), then they need to be declared a use of force. For example, if the descriptions by DoD and government officials about the scope and intensity of the physical damage inflicted by North Korea in the Sony cyber incident are accurate, it quite obviously meets the standard establish in the Koh speech, the *DoD Law of War Manual*, and Painter's testimony.[98]

---

96 Interview by Charlie Rose with James Clapper, Director of National Intelligence, in New York, N.Y. (Oct. 25, 2016), http://www.cfr.org/intelligence/conversation-james-clapper/p38426 [https://perma.cc/L3CA-V98R].

97 *See, e.g.*, Frank J Cilluffo and Sharon, Global Ransomware Attack Reinforces Message of Trump's New Cybersecurity Order, THE CONVERSATION (May 12, 2017, 3:51 PM EDT), https://theconversation.com/global-ransomware-attack-reinforces-message-of-trumps-new-cybersecurity-order-72239 [https://perma.cc/9ZCQ-LHV9] ("One crucial element that has been largely missing from American cybersecurity efforts so far is cyber-deterrence.").

98 Harold Honhgu Koh, Legal Advisor of the Dep't of State, International Law in Cyberspace,
Address to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), http://digitalcommons.law.yale.edu/fss_papers/4854 [https://perma.cc/5FFP-8RKM]; DOD LAW OF WAR MANUAL, *supra* note 46; *Digital Acts of War – Evolving the*

Watering down official characterizations of the Sony attack (where computers were "fried" and "thousands" of them rendered "inoperable") to merely being an incident of cybervandalism carries real consequences. At best, confusion arises, and at worst, a norm develops that gives potential cyber adversaries reason to believe that even if they inflict damage on that level, scale, and intensity, they will not face anything worse than an indictment in a U.S. court—that will never result in an actual prosecution.

To be sure, there are acts that may appropriately be characterized as solely cybervandalism. For example, in early 2015 when Islamic State hackers penetrated U.S. Central Command[99] social media accounts, the United States branded it as "purely a case of cybervandalism."[100] Even though the hackers posted "threatening messages and propaganda videos, along with some military documents," the command maintained that the "operation military networks were not compromised and there was no operational impact to U.S. Central Command."[101] Every hostile cyber activity cannot and should not be characterized as a use of force, even under the US's more permissive standard.

It does help when, as noted above, the United States specifically defines the cyber activities it wants to explicitly deter.[102] The problem with this is that it may include activities—cyber espionage for example—that are rightly violative of domestic U.S. law, but would not necessarily be something that the United States and its allies would want to be considered in

---

Cybersecurity Conversation: Hearing Before the Subcomm. on Information Security and National Security of the H. Comm. on Oversight and Government Reform, 114th Cong. (2016) (statement of Christopher M. E. Painter, Coordinator for Cyber Issues, U.S. Department of State).

99 U.S CENTRAL COMMAND, http://www.centcom.mil/ [https://perma.cc/L99T-6F7W].

100 Dan Lamothe, *U.S. Military Social Media Accounts Apparently Hacked by Islamic State Sympathizers*, WASH. POST (Jan. 12, 2015), https://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers [https://perma.cc/8RHQ-R46X].

101 *Id.*

102 *Report on Cyber Deterrence*, WHITE HOUSE (December 2015), http://1yxsm73j7aop3quc9y5ifaw3.wpengine.netdna-cdn.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf [https://perma.cc/77Z6-MDGV].

international law, at least at the moment, as a *casus belli*.[103] It may be suitable for the development of new norms[104] not involving force in light of the enormous capability of cyber methodologies, but a clear delineation between what authorizes a forceful response, and what is limited to other options is needed.

In short, for deterrence to work there needs to be more precision in the official language used to describe specific incidents that comports to the United States' own interpretation of a use of force that would authorize a response in self-defense.[105] If the facts show an incident being characterized as a use of force sufficient to permit the use of force under Article 51, then the official language needs to be consistent with that assessment.

B. Develop Norms for "Red Lines"

It is vitally important, however, to appreciate that simply because a particular cyber act may legally constitute an "armed attack" that might qualify for the political characterization of an "act of war," that does not necessarily mean that a country is obliged to respond to it with force. Indeed, there are many political reasons that would counsel against doing so. This is where Mr. Painter is mistaken in regards to his discussion about "strategic ambiguity."[106]

In deterrence, ambiguity may be useful with respect to a response, but it is markedly less so when you are talking about the threshold. Misunderstandings as to where the proverbial "red lines" are set can lead to dangerous miscalculation, unintended escalation, and unwanted conflict.[107] Given the enormous potential of cyber acts to do harm, potential actors ought not to get mixed

---

103 *Casus Belli*, BLACK'S LAW DICTIONARY (2d ed. 2017), http://thelawdictionary.org/casus-belli/ [https://perma.cc/LQ3J-SWT9].

104 WILLIAM BANKS, CYBER ESPIONAGE, SURVEILLANCE, AND INTERNATIONAL LAW: FINDING COMMON GROUND (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2558155 [https://perma.cc/G69G-W5HX].

105 Laura K. Bate, *In Search of Cyber Deterrence*, WAR ON THE ROCKS (Sep. 24, 2015), https://warontherocks.com/2015/09/in-search-of-cyber-deterrence/ [https://perma.cc/X54N-EEDD].

106 *See supra* note 98 and accompanying text.

107 Dot Wordsworth, *What, Exactly, is a 'Red Line?'*, SPECTATOR (Jun. 8 2013), https://www.spectator.co.uk/2013/06/that-red-line-were-not-supposed-to-cross-what-exactly-is-it/ [https://perma.cc/S7UK-P36Z].

messages as to how the United States considers harmful cyber activities.

Frustrations with the opaqueness as what cyber activity would constitute a *casus belli* appears to have motivated Congressman Mike Rounds to propose a bill earlier this year that would require the President to develop a policy for determining "when an action carried out in cyberspace constitutes an act of war against the [United States]."[108]

Rounds points to testimony of Marine Lt. Gen. Vincent Stewart, director of the Defense Intelligence Agency, as part of his rational for the legislation.[109] Stewart admitted that a "much fuller definition of the range of things that occur in cyber space [is needed], and then [we should] start thinking about the threshold where an attack is catastrophic enough or destructive enough that we define it as an act of war, I think that would be extremely helpful."[110]

Stewart is not alone in not "fully" understanding where the threshold lies. Other Pentagon leaders apparently are equally uncertain,[111] something that raises the obvious question: if our leaders do not know, how can we expect potential adversaries to understand which acts might spark a full-blown war? At the same time, except in the most aggravated cases, enumerating in advance precisely which cyber acts exceed the use of force threshold might be nearly impossible.

This is where norm development in international law comes into play. In developing norms, the United States needs to use the language of international law. Political terms like "digital acts of war" are unhelpful not only because they do not track with the language of the law, but because they also can imply to the general public a level of response that is unnecessarily provocative and even inconsistent with the proportionality and necessity factors intrinsic to a lawful exercise of self-defense, especially in the

---

108 Cyber Act of War Act of 2016, H.R. 5220, 114th Cong. § 1 (2016).

109 Mike Rounds, *Defining a Cyber Act of War*, WALL ST. J. (May 8, 2016, 4:08 PM), https://www.wsj.com/articles/defining-a-cyber-act-of-war-1462738124 [https://perma.cc/6KVT-479C].

110 *Id.*

111 Bryant Jordan, *US Still Has No Definition for Cyber Act of War*, MILITARY.COM (Jun. 22, 2016), http://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html [https://perma.cc/N68X-EXWP].

complex cyber arena.[112]

As discussed, the United States has, in fact, laid out in broad terms what kind of cyber activities it wants to deter, and generally how it interprets the law applicable to cyber operations.[113] What is required now is for the United States to act consistently with these conceptual positions when cyber incidents actually occur. We now seem to be in a cycle in which we are facing ever more dangerous and damaging cyber incidents, yet they are rarely given the appellations established U.S. legal interpretations would seem to require. Instead, incidents too often are characterized with language that would put them outside the kinds of activities that would authorize a forceful Article 51 response.

The United States also has to be more forthright about its response to incidents because that too influences norm development. True, there may be times, as the White House spokesman Josh Ernest said, that the United States would "never announce" a response to a particular cyber incident, but that should very much be the exception and not the rule.[114] As Bloomberg News' Eli Lake argued last July after the DNC hack:

> [T]here is also a consequence for keeping quiet. It might give Russian hackers the impression that the [United States] is uninterested in deterring them. Indeed, it appears they are under that impression already.[115]

Transparency should not be underestimated as a deterrence factor.[116] Potential cyber attackers calculate exactly what kind of malicious activity will generate a response, and how costly that response might be.

VII. The Bigger Picture

It is crucial that the United States unmistakably express its positions about cyber incidents it has suffered, particularly given

---

112 Terry Gill, *Anticipatory Self-Defense in the Cyber Context*, 89 INT'L. L. STUD. 438, 460 (2013).

113 *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 46.

114 Ernest Press, supra note 72.

115 Eli Lake, *Why Russia Keeps Getting Away With Hacking America*, BLOOMBERG (Jul. 31, 2016, 10:30 AM), https://www.bloomberg.com/view/articles/2016-07-31/why-russia-keeps-getting-away-with-hacking-america [https://perma.cc/HGW3-VH5K].

116 Laura K. Bate, *In Search of Cyber Deterrence*, WAR ON THE ROCKS (Sep. 24, 2015), https://warontherocks.com/2015/09/in-search-of-cyber-deterrence/ [https://perma.cc/Q4XL-97Y5].

the approach of two of the world's most formidable cyber actors. Professor Schmitt noted in 2014 that:

> The UN Group of Governmental Experts, which includes representatives from Russia and China, agreed in 2013 that international law applies to cyberspace. Interestingly, Russia and China did not agree to a reference to international humanitarian law and China reportedly does not accept the applicability of IHL in cyberspace.[117]

For example, the Chinese acknowledge that "although the existing laws on armed conflicts and general international principles may all apply to cyberspace, there are still many issues that need clarification . . . [t]he international community should, therefore, revise existing laws[—]but it is important that this international legal framework maintains sufficient openness and flexibility."[118]

Although purportedly not officially speaking for the Chinese government, Professor Huang Zhi Xiong of China's Wuhan University Institute of International Law is reported to have shared the opinion that:

> In his view, the Tallinn factors relevant to evaluating when a cyber activity rises to a use of force (which include severity, directness, and invasiveness) are too malleable and the bar for what activities are uses of force should be higher. Second, he sought a higher bar than Tallinn 1.0 sets for when a state may invoke the right of self-defense. In his view, a state does not have a right of self-defense against attacks by non-state actors, nor does a state have the right of self-defense against an imminent attack.[119]

If the Chinese government de facto adopts (or has already adopted) Professor ZhiXiong's view as to the inapplicability of the right to self-defense in cyber incidents, and Russia fuses with that view, their combined impact would be very influential in the development of an international norm that is contrary to the U.S. view.

---

117 Michael M. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 271 n.7 (2014) (citation omitted).

118 Li Zhang, *A Chinese Perspective on Cyber War*, 94 INT'L. REV. RED CROSS 801, 804 (2012).

119 Ashley Deeks, *Tallinn 2.0 and a Chinese View on the Tallinn Process*, LAWFARE (May 31, 2015, 2:00 PM), https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process [https://perma.cc/L8QD-STXR].

VIII. Conclusion

It is inarguable that the United States needs to be judicious in its characterizations of, and responses to, cyber events.[120] No one wants to unnecessarily aggravate an already difficult situation. Uncertainty as to how to effectively respond and still avoid counterproductive escalation is a real problem of deterrence. But before determining whether and how to respond, the legal options need to be apparent. In that regard, the United States is at the point where it needs to be more forthright when incidents occur that appear to violate its own announced standards as to when a cyber action equates to an "armed attack."

Again, calling something the equivalent of an "armed attack" so as to permit a forceful and proportional response in self-defense under Article 51 does not mean that such action would necessarily be forthcoming in every instance. Rather, it would make it unmistakable to all concerned that the United States asserts it has a lawful option to use force in self-defense if it chooses to do so, not that it will in each case.

As the United States fails to properly characterize cyber incidents, and frequently suggests that they are simply vandalism, thefts, or other matters which are readily interpreted by cyber actors and publics around the world as being within the law enforcement modality and outside of the jus ad bellum legal regime, no one should be surprised if norms begin to emerge more in keeping with what Russia, China, and hostile cyber actors prefer.

Deterrence in the cyber realm quite obviously needs strengthening, and dealing with the legal piece of that effort matters. We still have the chance to set the record straight—to develop that "body of law," Director Clapper believes we are missing—but that opportunity diminishes with each passing incident where the proper legal characterization is understated and muddled.

---

120 Trevor Timm, *If the US hacks Russia for Revenge, That Could Lead to Cyberwar*, GUARDIAN (Oct. 19, 2016, 11:17 AM), https://www.theguardian.com/commentisfree/2016/oct/19/russian-hacking-us-retaliation-cyberwar-international-treaty [https://perma.cc/FQ79-8HEC].