ISSN: 2582 - 2942

LEX FORTI

LEGAL JOURNAL

VOL- I ISSUE- VI

AUGUST 2020

ISSN: 2582 - 2942

DISCLAIMER

ISSN: 2582 - 2942

EDITORIAL BOARD

ISSN: 2582 - 2942

EDITORIAL BOARD

ISSN: 2582 - 2942

ABOUT US

LexForti is a free open access peer-reviewed journal, which gives insight upon broad and dynamic legal issues. The very objective of the LexForti is to provide open and free access to knowledge to everyone. LexForti is highly committed to helping law students to get their research articles published and an avenue to the aspiring students, teachers and scholars to make a contribution in the legal sphere. LexForti revolves around the firmament of legal issues; consisting of corporate law, family law, contract law, taxation, alternative dispute resolution, IP Laws, Criminal Laws and various other Civil issues.

Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions

Naveen Gupta And Kriti Gera

INTRODUCTION

When is a cyber-attack (or a cyber-attack threat) giving rise to a right of self – defense – including armed self-defense and when will it be? By "cyber-attack" we mean the use of malicious programming code or electronic signals to modify, interrupt, weaken or damage programming or network systems or the information or programs on them. It is widely believed that sophisticated cyber-attacks can inflict massive damage – whether to military resources, economic and financial structures, or social functioning current dependence on interconnectivity in the network, although how vulnerable the United States and its allies are to these attacks is strongly contested.[1]

This article explores these issues through three lenses:

1) A legal perspective to explore the spectrum pf permissible definitions of self-defense rights as applied to cyber-attacks and the relative merits of definitions within that context;
2) A strategic perspective to relate a supposed right of armed self-defense to long-term policy interest like security and stability and
3) A political viewpoint to understand the context in which the government decision-makers will be faced with these problems and predictive decisions on the reactions of prominent actors to cyber crises; International System.

Our key argument is that these three viewpoints are interrelated so that lawyers involved in addressing these questions can include their study in strategic and political aspects. It is not just about getting it is banal, commonplace, that policy, strategy, and law are interrelated to. They are course. Rather, this article aims to demonstrate precisely how policy, strategy and law creation is likely to play out interdependently on this particular threat-cyber-attacks- and draw some conclusions from that study on legal growth in this field.

This paper focusses on military self-defense against cyberattacks that is, legally self-defense is not intended to imply that this is the most important part of a holistic information security strategy – far from it. Most attention these days is rightly centered on other components of the strategy including enhanced network security and "attack" Cyber initiatives, while military action forms part of the strategic instrument package. A significant point is also that this study is formed with an American viewpoint of its own record. Nonetheless, if one believes, as we do that legal research

[1] See Mark Clayton, The New Cyber Arms Race, CHRISTIAN SCIENCE MONITOR (Mar. 7, 2011), http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-armsrace. Some experts warn of a "digital Pearl Harbor" or other likely devastating attacks on the United States. See, e.g., Mike McConnell, To Win the Cyber-War, Look to the Cold War, WASHINGTON POST, Feb. 28, 2010, at B1. Other experts, however, argue that these risks are greatly exaggerated. See, e.g., Thomas Rid, Cyber War Will Not Take Place, 35 JOURNAL OF STRATEGIC STUDIES 5 (2012).

and growth and cannot be separated from policy and politics, then America's strength-in its multiple forms- and susceptibility to strength will greatly influence its own interpretive approach to these issues, and it will greatly influence international legal action in this field because of its relative power globally

LEGAL PERSPECTIVE

Within the jus ad bellum system, a legal viewpoint on the issue of cyber threats as armed attacks sees the issues as one of the self-defense rights. Article 2(4) of the UN Charter stipulates that all members shall refrain from threatening or using force against the territorial integrity or political independence of any state or in any other way incompatible with the interests of the United Nations in their International relations. Section 51 however, states that there is nothing in this charter to hinder the inherent right to individual or collective self-defense if an armed attack occurs against a member to the United Nations. A legal question then arises; when, if ever, is a cyber-assault an 'armed attack' that causes the right of self-defense?

There is no consensus answer to this question yet and there are several analytics the methods contend with the adherents. A strict reading of "armed-assault" would restrict its scope to kinetic aggression, as opposed to non-physical violence or damage without physical harm (taking economic or diplomatic sanctions, for example), and cyber-attacks may, therefore, be treated as unable to cause armed self-defense rights on their own. This position provides a bright-line rule that is relatively easy to apply but the treatment of chemical or biological weapons attacks (which would be recognized by everyone as an armed attack) is difficult to cope with and does not account for new cyber vulnerabilities[2]. Therefore, the position that cyber-attack could never constitute an armed attack is rarely advanced.

A more traditional starting point for research is taking into the account the results of the implications of cyber-attack on how it crosses the "armed-assault" threshold. That is, the nature of a "gun assault" and resulting right to self-defense is the direct or even indirect outcome of a hostile activity- usually, but not always, in the form of kinetic violence- and legal analysis should be carried out by analyzing whether the effects of a specific cyber assault are reasonably close to kinetic violence.

A further division in strategy is among those who follow an effect-based approach to Article 51. Several legal experts have indicated that a cyber-assault must have violent implications if it is to

[2] . This essay draws heavily on a previous article: Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), 36 YALE JOURNAL OF INTERNATIONAL LAW 421 (2011).

count as an armed-attack produced usually with bombs or bullets[3]. So for instance a cyber –attack had a power station exploded or one that caused aircraft to crash might technically constitute an armed-attack, but cyber-attacks that cause economic or social damage-such as stock market shutdown or stoppage of transport systems-could not be authorized. Numerous other legal experts take it a wider view of what kind of consequences could constitute an armed assault, arguing that focusing on death or physical harm does not compensate for the vital dependence of modern society on information and communications infrastructure[4]. Therefore, they should look beyond just the form of impact to their magnitude, immediacy, and other considerations in the assessment of a cyber-attack cross the threshold of self-defense.

Any interpretive approach based on effects leads to difficult secondary situations. These include how to quantify the proportionality of an armed response (especially given that it may be difficult to measure the effects of cyber-attacks and it may be difficult to determine direct causality); when to judge imminence for anticipatory self-defense purposes (due to this discernment cyber threats from other cyber operations[5], such as hacking, are so complicated because certain sequences of threats take place in split seconds) after they are launched; and how to understand state liability (because attacks can be initiated by individuals or groups with loose links with States).

In general, the United Nations government has adopted ab effect based-approach, but only slowly publicly offering information about how it does or legally determine the consequences of cyber-attacks. Testifying before the Senate committee that he is considering his nomination to head the new United States[6]. Lieutenant General Keith Alexander Cyber command, explained "there is no international consensus on an accurate definition of the use of force, whether in or out of cyberspace. Individual nations may, therefore, claim various meanings and apply specific criteria to what constitutes the use of force. He went to say that if the president decides[7] that a cyber-incident meets the threshold of using force/ armed assault, he may decide that the activity is of

[3] U.N. Charter art. 2, para. 4.
[4] Id., art. 51.
[5] For a discussion of these positions, see Oona A. Hathaway et al., The Law of Cyberattack, 100 CALIFORNIA LAW REVIEW 817, 841–49 (2012).
[6] See NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 33–34 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT]; Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thought on a Normative Framework, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 914–15 (1999); Katharina Ziolkowksi, Computer Network Operations and the Law of Armed Conflict, 49 MILITARY LAW & THE LAW OF WAR REVIEW 47, 69–75 (2010); TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 92–95 (Michael N. Schmitt ed., 2013), draft available at http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft /1#share.
[7] See, e.g., Yoram Din stein, Computer Network Attacks and Self-Defence, in COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (Vol. 76, U.S. Naval War College International Law Studies).

such nature, length or severity as to warrant the exercise of our right to self-defense and/or the initiation of hostilities as a suitable response".

More recently, in its official cybersecurity policy, the white house declared that consistent with the Charter of the United Nations, states have an inherent right to self-defense which can because of some hostile actions in cyber-space. He went on to state:

The United States will respond, if necessary, if aggressive actions in cyberspace just as we would to any other threat to our country. All States have an inherent right to self-defense and we recognize that some aggressive acts carried out through cyberspace may force actions within the commitment we have with our partners in the military treaty. We reserve the right to use all means available- diplomatic, analytical, military, and economic- as required and consistent with applicable international law to protect our country, our allies, our partners, and our interests.

While expressly endorsing an effect-based legal theory or specifying the specifics of that study, the United States appears hereby to depend on it in claiming the same the widely accepted self-defense authority as applied to traditional armed attacks. As for every gun attack, the United Nations announces that it finds that all cyber-threats open up the entire number of self-defensive tools[8]; cyber-threats would not automatically be met with responses limited to the cyber domain or other armed-force actions.

Providing a little more clarity on its legal stance on this, in 2011 the United States has explained to the UN Group of Global Experts its interpretation of Article 51 in the following terms[9]:

It can be hard to arrive at a definite legal conclusion as to whether a Disruptive cyberspace behavior is an armed attack that triggers the right to self-defense. These ambiguities and scope for dispute, however[10], do not indicate the need for a modern, precise, cyberspace legal system. Alternatively, they clearly represent the problems that occur in many ways when implementing the Charter Framework.

Nevertheless, the U.S. declaration concludes that "a disruptive activity in cyberspace could constitute an armed attack under some circumstances."

---

[8] See NRC REPORT, supra note 6, at 253–54 (arguing that the traditional legal emphasis on death or physical damage is problematic because "modern society depends on the existence and proper functioning of an extensive infrastructure that itself is increasingly controlled by information technology," and that therefore "[a]ctions that significantly interfere with the functionality of that infrastructure can reasonably be regarded as uses of force, whether or not they cause immediate physical damage").

[9] Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command: Before the S. Armed Services Comm., 111th Cong. 11 (Apr. 15, 2010), http://www.armed-services.senate.gov/statemnt/2010/ 04%20April/Alexander%2004-15-10.pdf.

[10] Id. at 12.

State Department Legal Adviser Harold Koh commented a little more on the U.S. stance in a public address in September 2012, stating that such cyber-attacks may constitute a prohibited use of force:

Cyber activities that lead to death, injury, or substantial destruction would likely be viewed as a use of force[11]. To determine if an incident was a use of force in or across cyberspace, we need to evaluate factors including:

The context of the event, the actor perpetrating the action (recognizing the challenges of attribution in cyberspace), the destination and location, the effects, and the intention, among other possible issues. Examples of cyber-crime that would constitute a use of force are widely cited, for example:

1) Operations triggering a nuclear power plant meltdown;
2) Operations opening a dam above a populated area causing destruction; or
3) Operations disabling air traffic control resulting in airplane crashes.

He clarified the long-standing position of the United States that any such use of force would theoretically cause self-defense protection as an armed attack[12].

At the time of writing, some U.S. allies were wary of moving in this general direction has been expressed through public declarations, while other powerful States have a concern about it. The British for example, in 2012 in response to the parliamentary questions, the Minister of the Armed Forces claimed that a cyber-attack like the one that Estonia experienced in 2007[13]- which was widely blamed on Russia and caused major economic disruption- might trigger the collective self-defense provisions of NATO. NATO as a global party operated on a collaborative approach to cybersecurity, while NATO's official self-defense language was very cautious. In 2011, the U.S. and Australia announced that their Mutual security treaty applies to cyberspace, reflecting a shared agreement to handle the cyber-attacks within the same cooperative context as armed threats but without specifically leading to an armed response. Meanwhile, China rejected the idea that cyber-attacks could cause a conventional right of self-defense in diplomatic groups, preferring new forms of international law and a wider view of cyber threats to be included Internet content which threatens to stabilize the regime, Russia

[11] THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 10 (2011).
[12] Id. at 14.
[13] See U.N. Secretary-General, Replies to the Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the U.N. Secretary-General 18, U.N. Doc. A/66/152 (July 15, 2011).

has championed an international deal to fill up what it sees as, Gaps in international cyber-weapons legislation.

Following calls from some quarters[14] that they are urgently seeking direct resolution, legal questions regarding cyber-attacks as armed attacks are likely to be addressed not by formal, multilateral instruments-like a new treaty convention- but incrementally by state practice. That is, though the prevailing behavior and legal[15] views expressed by states in planning and responding to cyber-attacks incidents, the law will evolve and adapt with time.

This means that legal growth is likely to take place in a large proportion via the theory of proactive planning and declaratory policies released in anticipation of real cyber-attack crises[16], we need to change our analytical lens to a strategic viewpoint. In addition to the unilateral and joint self-defense policy declarations cited earlier, for example, Japan's national security authorities apparently followed the U.S. lead, largely adopting 51 on cyber threats while preparing their protection. Keeping in mind the dependency on Japan U.S. security assurances are not that shocking and demonstrate the tightness linking legal development to strategic relationships[17].

Legal growth is often likely to result in gradual behavior and the responses of states and other major international players during and after the real cyber-attack crisis[18]. This means which we will also have to tilt our theoretical lens toward a political perspective.

A STRATEGIC PERSPECTIVE

A strategic viewpoint on the topic of cyber-attacks as armed attacks sees the topic as one that ties a supposed right to armed self-defense to long-term political interest- both national and global in the case of the US- including security and stability[19].

Armed self-defense against cyber threats can be of strategic benefit in many values. Firstly, there may be anticipatory or sensitivity military behavior in certain situations, the security of

[14] Id.
[15] Id
[16] Harold Hongju Koh, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012), http://www.state.gov /s/l/releases/remarks/197924.htm (emphasis in original).
[17] See UK Minister: Cyberattack Could Prompt NATO Action, GUARDIAN (May 16, 2012), http://www.guardian.co.uk/world/feedarticle/10245167.
[18] See NORTH ATLANTIC TREATY ORGANIZATION, STRATEGIC CONCEPT FOR THE DEFENCE AND SECURITY OF THE MEMBERS OF THE NORTH ATLANTIC TREATY ORGANIZATION ¶ 19 (2010), available at http://www.nato.int/lisbon2010/strategic-concept-2010- eng.pdf (discussing the need to develop joint policies on cyber defence).
[19] See Media Note, Office of the Spokesperson, U.S. Department of State, U.S.- Australia Ministerial Consultations 2011 Joint Statement on Cyberspace (Sept. 15, 2011), http://www.state.gov/r/pa/prs/ps/2011/09/172490.htm.

military and vital infrastructures is necessary the susceptibility to cyber-attacks for example, by striking at installations or individuals responsible for initiating or guiding them- although since the physical infrastructure associated with cyber-attacks can be very small and widespread[20], this kind of proactive use of force primarily to neutralize the risk of initial or subsequent cyber-attacks has not been the subject of much debate. Second, the credible threat of self-defensive military actions may help to discourage cyber-attacks by increasing the prospective costs of aggressive cyber operations in the minds of adversaries (although possibly not so much of non-state adversaries, against whom deterrent threats of military action would not be very potent). The U.S. declaratory positions mentioned in the previous section are likely to underlie these strategic rationales, notifying adversaries that they should expect a potential military response to such cyber threats.

This is not the place to address the particular issues in-depth and Nuances of partially depending on the military security of cyber deterrence attacks, a subject written down, in-depth by several others. The key issue here is the manner in which-turning our lens back a bit and widening the aperture to pull together the legal and strategic viewpoints-certain cyber threats to constitute an armed assault might make a strategic contribution. In a number of ways, it could do so.

For instance, if you think that armed self-defense is important protecting against cyber-attacks by means of anticipatory or responsive military actions, internally a well-established legal right helps to strengthen the hands of political leaders who weigh such options (an issue that was further discussed in the next session, turning our lens towards a political perspective). An established or articulated right gives legitimacy to powerful options and can be taken as a guide to likely global reactions. A well- established right also promotes military readiness for these contingencies by removing internal hurdles and increasing the authority and institutional requirements to do so. It is much easier to operate inside organizations tasked with operationalizing them to develop and plan policy route options which are considered legal.

Through thinking externally about others' standards, a legal right to armed self-defense may contribute to the dissuasion by creating and to more firmly and explicitly express red lines associated with self-defensive attacks. This helps signal other thresholds outside of which we should foresee big escalation, involving big means. Combined with the rules of state duty, a right of armed self-defense may also encourage states to crack down more strongly on cyber-

[20] See Adam Segal & Matthew Waxman, why a Cybersecurity Treaty Is a Pipe Dream, CNN (Oct. 26, 2011, 2:01 PM), http://globalpublicsquare.blogs.cnn.com/2011/ 10/27/why-a-cybersecurity-treaty-is-a-pipe-dream/.

attacks launched from territories on cyber threats within their jurisdiction, whether out of a sense of legal obligation or fear of being attacked with armed self-defense[21].

However, those strategic benefits need to be balanced with strategic risks legally associated with the prosecution of such cyber threats as armed attacks. Calibrating between these benefits and risks has always been an aim and a cornerstone of the jus ad bellum system, and it will be particularly difficult to adapt it to this area.

One competitive danger is the ability to erode regulatory restrictions on fighting, focusing our attention back onto the legal perspective. Since the capacity of state and non-state actors to carry out different kinds of malicious, aggressive or intelligence-gathering activities in cyberspace is proliferating, the deterrent advantage of treating them as armed attacks that cause self-defense protection under Article 51 may be outweighed by the dangers of the legal barriers to military action in a wider range of circumstances or conditions. In reality, some may argue that the strategic benefit of promoting a right to self-defense against cyber-attacks may turn out to be very low- because, among other reasons mentioned in the following section, it may be very difficult to show publicly enough that one's case merit military responses- in doing so, it could lead to greater insecurity and instability of the international system by eroding the regulatory limitations on armed responses to non- military damages[22].

The strategic threat is the miscalculation of escalation: perhaps we want the law to help remain in the hands of the leader who may be prone to violently overreact to the cyber crisis. Rather than settling International law may play a role-normatively and bureaucratically- in fostering more rigorous deliberation for decision-makers encouraging strong responses, even if one doubts that it places absolute restrictions on powerful states in severe circumstances. This indicates once again the need to think of the policy of the cyber-attacks as armed attacks while still looking at the topic through a political lens.

A POLITICAL PERSPECTIVE

A political viewpoint considers the context in which the political situation decision-makers will face these issues and predictive judgements regarding the reactions of influential actors in the international systems to cyber-attack crisis. There is no doubt that the politics of cyber-

[21] See Govt Claims Cyberdefense Right: Says International Laws Should Be Applied to Computer Infilitration, DAILY YOMIURI ONLINE (May 17, 2012), http://www.yomiuri.co.jp/ dy/national/T120516005387.htm.
[22] See NRC REPORT, supra note 6, at 256 (discussing costs and benefits to preventing escalation in setting an appropriate threshold for self-defence).

attacks will be influenced by law and strategy in this area, but no successful legal or strategic theory can be established that does not account for politics.

In a possible cyber crisis, domestic and foreign affairs are of unable to predict correctly, course. Nonetheless, a few aspects of these situations are also likely to affect such policies. Next, cyber-attack events would likely include a collection of publicly unclear facts. Conventional military assaults are typically very visible-kinetic aggression can and is frequently transmitted widely, instantly and understandably- and their widespread history allows political responses relatively predictably (though far from entirely). In comparison, malicious computer code or behavior in cyberspace is elusive in public opinion, is technically quite complex, and are likely to emerge piece worthy.

Second, and closely linked, responses to cyber-attacks and reactions are likely too high levels of government secrecy. Cyber-attackers may seek to keep their roles and strategies hidden. Nevertheless, defenders may also be unwilling to reveal information or even the very nature of cyber-attacks, whether to protect secrets about their weaknesses and defenses, avoid public hysteria, avoid political embarrassment or escape unnecessary domestic pressure to take retaliatory action[23]. Trying the case of Stuxnet and other cyber-attacks on Iran's nuclear development program; press reports claim that the U.S. and Israel conducted such attacks covertly- trying not just to hide their liability but to conceal the very presence of a cyber-attack- while Iran officially denied that it had been targeted or suffered any substantial harm.

Second, cases of cyber-attack may entail difficulty in verifying the attribution. It is fiercely debated how effectively states can track digital fingerprints of cyber-attacks, which can be redirected back to their ultimate source via the computer systems of many unsuspecting third parties and it is commonly assumed that some states will carry out cyber-attacks via loosely connected or unofficial private parties. These attribution problems can be overstated as a strictly technical matter, especially for the United States and its leading intelligence and cyber-forensic capabilities. Nevertheless, as a political issue, a crucial question is whether attacked states or their allies can demonstrate adequately the aggressor's guilt against domestic and foreign audiences to justify armed self-defense. There could be a substantial difference between adequately defining internal intelligence attribution intent and do so to explain forceful responses externally.

[23] See David E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, NEW YORK TIMES, June 1, 2012, at A1.

A political consequence of these factors is the armed self-defense to a cyber-attack will probably require a fairly high minimum harm threshold-probably a much larger amount of harm than would be required if a conventionally armed attack were to occur. Political decision-makers may find it very difficult to mobilize support at home and abroad for military responses to individuals' cyber-attacks that do not inflict serious and publicly discernible harm, while legal arguments that reinforce their hands. While even low levels of violent kinetic aggression talk of a barrage small missile that doesn't detonate or cause a lot of injuries- not only justify an armed response strategically, dud or stymied cyber- attacks probably won't be. Turning back to the legal perspective, this means that while legal line drawing close to the margins is very challenging for lawyers applying an effect-based analysis, it may not be appropriate. This is very problematic in practice since states are unlikely to react with military force to small-scale attacks.

That said, it is also possible that the cyber-attacks are very dangerous for which Armed self-defense is a choice that will occur in or against the context it is paired with other offensive practices. To put it another way, and think even from the strategic viewpoint, there are potentially few "naked" instances of Cyber assaults — bolts from the blue in the complete absence of any substantial aggressive acts or threats — against which political leaders would find armed self-defense a viable response. Cyber-attacking states are likely to do so in tandem with other strategic actions, including military-threatening moves. Non-state groups, for example, terrorists

That aggression has usually already been committed by organizations to which military self-defense might make little sense. Regardless of how they do it Non-cyber actions and attacks officially fall within the legal structure of a defending State Research, they would certainly factor significantly in the public justification of force as a political matter.

CONCLUSIONS

As the question of cyber-attacks as armed attacks is explored simultaneously through the three lenses-legal, strategic and political-What emerges are general assumptions. Firstly, there is a variety of plausible definitions of cyber "armed attacks" to cause military action for the near future good self-defense and a secure majority are impossible[24]. One explanation for this legal

[24] On some of these asymmetries, see Thomas Rid, Think Again: Cyberwar, FOREIGN POLICY, Mar.–Apr. 2012, at 58.

uncertainty is that strategic asymmetries are drawn Interpretation of different ways. We have mentioned it this way before:

The United States appears to be putting its legal bets on a potential world where it will continue to rely partly on its comparative military superiority to discourage cyber-attacks while supplementing the deterrence with its own offensive, defensive, and pre-emptive cyber-capabilities — a gamble the plays to some advantages but also carries risks. Reaching a substantive agreement with Certain major powers on these topics would be partly difficult, as they Perceive a particular combination of competitive prospects and risks. US lawmakers should also be prepared to work within a deeply contested and unpredictable international legal climate.

Legal positions among states[25] — and even within states — may change As the offensive benefits and defensive weaknesses change over time. In addition, international law controlling force is gradually evolving, whilst the information technology that produces such strategic opportunities and threats will continue to develop rapidly.

Second, gradual legal progress by State practice will be especially difficult to determine because of many characteristics of cyber-attacks Actions and counteractions with respect to cyber-attacks will lack the consistency of most other types of conflict, often for technological reasons but often for political and strategic reasons. It will be hard to establish consensus understandings, even of the factual trend's Legal claims and counterclaims of States are founded on the presumption that these arguments are openly made because too many of the key facts are disputed, hidden, or difficult to ascertain or quantify. In addition, the probable infrequence Within the background of other threats or active conflicts, "naked" cases of cyber-attacks mean that there will be few opportunities to establish and analyze State practice and reactions to them in ways that set a broadly applicable precedent.

Finally, legislation can and should be used to endorse calibration strategy Suitable causes and self-defense thresholds, while political ones the dynamics of cyber-attack crises – many of which are directly related to the technological features of cyber-attacks – make it more difficult to do so in advance than traditional military threats did. This means changing international law and developing amongst allies and Policy alliances for fighting cyber threats go hand in hand. Some who follow a more formalistic method of self-defense law that consider this approach to legal interpretation as too malevolent and subordinate to politics of power. Yet

[25] Waxman, supra note 2, at 448–49.

any legal solution that refuses to account for cyber-attacks strategic and political complexities is unlikely to withstand early encounters with those realities.