No. 1

Game of Code

The Use of Force Against Political Independence in the Cyber Age

By Major Chris H. Kinslow

Every American should be alarmed by Russia's attacks on our nation. There is no national security interest more vital to the United States of America than the ability to hold free and fair elections without foreign interference.[1]

It is the middle of March. You are making one final trip to the grocery store for last-minute party supplies prior to what will certainly be a well-deserved Patriumland Independence Day feast. Patriumland is a new country, about the size of Rhode Island, emerging ten years ago after the partial breakup of two neighboring countries. It is a constitutional democracy. The independence that you now celebrate was the result of the will of Patriumland's proud people.

Your feast is well-deserved because you have just endured six months of constant political rhetoric between several different presidential candidates. The election was extremely divisive, pitting brother against sister, mother against daughter. Many citizens were concerned that a peaceful transfer of power might not occur. In the end, one candidate emerged victorious, and the others conceded defeat. The country, proud and resilient, began stitching up those ripped relationships. Suddenly, your phone vibrates erratically in what could only be a breaking "push" notification from your Patriumland Daily News smartphone application. You quickly check the headline and immediately know that you will forever remember where you were when you learned that foreign hackers usurped the people's true choice for president.

In the days that follow, Patriumland's security agencies ascertain that a rival nation planned and directed a cyber operation that hacked into Patriumland's electronic voting system and actually changed votes to reflect that nation's presidential pick. Several members of parliament have called for a military response.

The threat of an operation like the one in fictional Patriumland is real.[2] As elections move toward increased use of cyberspace, including such mechanisms as electronic voter registration and voting, the danger increases that a cyber operation will manipulate the election process.[3] A foreign power's capability to install its choice of political candidate without firing a single conventional weapon necessitates a hard look at the interpretation and application of international law governing intervention in a country's political independence. The international community should adopt the concept that certain foreign cyber operations conducted against a state's political independence can rise to an armed attack, thereby allowing a military response as part of a state's right of self-defense. As such, existing tests used to determine whether a particular act qualifies as an armed attack must be updated to reflect the realities of current methods of force.

Many U.S. officials recognize the potential threat, as evidenced both by a recent Senate Armed Services Committee hearing[4] and by the Office of the Director of National Intelligence and the Department Homeland Security in the following statement: "The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of emails from U.S. persons and institutions . . . [with the intent] to interfere with the U.S. election process . . . . We believe . . . that only Russia's senior-most officials could have authorized these activities."[5]

Considering emerging cyber threats, this paper evaluates under what conditions a state could consider intervention in the political process to be the equivalent of an armed attack. Section II provides background on the topic's international law framework. Section III continues by discussing interference with political independence. Section IV introduces the effects-based test and looks broadly at the Department of Defense's (DoD) position on cyber operations as potential armed attacks. Finally, Section V addresses the concepts of force and self-defense as applied to cyber operations targeting political independence and suggests a test that officials might use to determine whether a particular incident of intervention constitutes an armed attack, thereby opening avenues for the use of force—either through self-defense or by United Nations (UN) Security Council resolution under the UN Charter.

II. Background

Scholars have devoted a significant amount of academic research to determining what constitutes the use of force and an armed attack in the law of armed conflict—including in the context of cyber operations.[6] Although this paper is concerned directly with the narrow subset of emerging cyber operations affecting political independence, there are established rules regarding the use of force in international law that guide the discussion.

A. The Use of Force

The UN came into existence in the wake of two world wars with one of the express purposes in its charter being "to save succeeding generations from the scourge of war."[7] To that end, the drafters set out a baseline rule in Article 2(3) of the UN Charter requiring that states use peaceful means to resolve disputes.[8] Building upon that concept, Article 2(4) of the UN Charter goes on to direct that states "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[9]

Breaking the clause down to address the hypothetical situation in Patriumland, the key terms are "use of force" and "political independence".[10] It seems simple enough to say that a nation using force against another nation's political independence is a violation of Article 2(4) of the UN Charter.[11] However, the drafters provide no definition within the Charter for this seemingly broad classification of actions that could violate the use of force standard, and consequently, much confusion and debate has ensued in subsequent years.[12] Political independence, too, is left undefined, and visions of a foreign army marching into a nation's capital must be reconciled with the reality of less obvious exercises of this type of interference.[13]

Even if the practitioner is able to articulate an argument that an act was an illegal use of force, there is no flow chart in the Charter directing the reader to a follow-on page for further instructions.[14] There are, however, two provisions in the UN Charter that clearly provide exceptions to the prohibition on the use of force contained within Article 2(4).[15] First, Articles 39 and 42, respectively, authorize the Security Council to: (1) classify a state's activities as acts of aggression or threats and breaches of the peace; and (2) further determine whether armed forces are necessary to maintain or restore peace.[16] Since the UN Charter is designed to maintain world peace, the five permanent members of the Security Council[17] have veto authority against any potential resolution involving, among other things, a use of force.[18] As such, political and ideological alignments may make it extremely difficult for a state to secure a Security Council resolution authorizing the use of force.

Article 51 of the UN Charter provides a second rationale for the legal use of force by preserving a state's right to self-defense after falling victim to an armed attack.[19] Notably, the plain text of Article 51 does not grant an *authority* to use force.[20] Rather, it restricts the Charter's applicability over instances of a state's exercise of the "inherent right of . . . self-defense."[21] However, as Article 51 can be reasonably read to limit a state's use of force in self-defense preconditioned upon an event of certain magnitude, that event being an armed attack, lawyers and diplomats have spent considerable time attempting to delineate the parameters of what constitutes an armed attack.[22]

A primary point of contention within international law is whether all uses of force are armed attacks.[23] One argument is that there is no difference between the two, while the other argues that use of force is a large category of activities containing a smaller subset of events that qualify as armed attacks.[24] This difference between the two interpretations results from whether the gravity of a use of force determines when an armed attack occurred.[25]

Another important concept for understanding the rights preserved by Article 51 is a state's ability to legitimately use force under a self-defense rationale when faced with an imminent threat. Adherents to this principle of customary international law assert that the UN Charter did not restrict the customary right of self-defense to situations where an attack has already occurred.[26] The test advocated by then-Secretary of State Daniel Webster regarding the *Caroline* incident is generally cited as the embodiment of the principle of anticipatory self-defense.[27] It states that the threat must be "instant, overwhelming, leaving no choice of means, and no moment of deliberation."[28] In contrast, current U.S. policy on self-defense is that the use of force may be necessary after exhaustion of reasonable peaceful means and that it be proportionate to the threat.[29] This is regardless of whether an attack has or has not yet occurred.[30]

B. Cyber Operations

Traditional instruments of employing force are joined today by cyber threats, which nations are working to address through the law of armed conflict. Under DoD policy, cyber operations are defined as "[t]he employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[31] Some examples of cyber operations include intelligence

gathering, gaining access to a network, and introducing malicious code for immediate or future use.[32]

Other activities within cyberspace that do not have a purpose of "achieving objectives or effects" are not considered cyber operations under U.S. policy.[33] These activities include such things as broad information distribution, air traffic control, and facilitation of command and control operations.[34] Likewise, targeting an adversary's cyberspace capabilities through non-cyberspace methods would not be considered a cyber operation.[35] United States policy accepts that cyber operations may constitute forcible or non-forcible means, depending both upon the type of operation and the operation's effect.[36]

III. Political Independence and Interference

As previously discussed, it can be difficult to determine when actions qualify as uses of force against political independence and when those uses of force equal an armed attack. Although the concept of political independence is broad, defining it will limit the field of potential interventions that may be included for analysis. In treaty law, Article 3 of the *Montevideo Convention* provides a detailed description of what might be described as the concept of political independence: "[T]he state has the right to defend its integrity and independence, to provide for its conservation and prosperity, and consequently organize itself as it sees fit, legislate upon its interests, administer its services, and to define the jurisdiction and competence of its courts."[37]

In her article concerning non-forcible interference in domestic affairs, Lori Damrosch defines political independence as "respect for the political freedoms of the target state's peoples."[38] She contends, however, that the concept of political independence "should be understood against the backdrop of the political rights of its inhabitants."[39] Under this conceptual framework, what comprises political independence in a democracy will differ from that of an autocratic society.[40] In the former, the native population's will is primary to the political process by design, whereas in the latter, the political destiny of the country is controlled by a limited number of individuals.[41]

Drawing from these concepts, for the purposes of this paper, political independence in a democracy is defined as the population's meaningful self-determination of its own government. Interference in that self-determination may manifest itself in a wide spectrum of both forceful and non-forceful foreign activities. Propaganda designed to influence public opinion, covert operations to replace government officials through peaceful means, training of antigovernment militias, and invasion by a hostile army are just a few of many potential examples of interference in political independence.

It can be difficult to determine when actions qualify as uses of force against political independence and when those uses of force equal an armed attack.

A. Intervention as a Violation of International Law

Understanding the concept of political independence, it is helpful to attempt to delineate the left and right limits of interventions in that political independence that might constitute violations of international law—taking into account not all interventions that violate international law are uses of force. Looking again to the *Montevideo Convention*, it provides, "No state has the right to intervene in the internal or external affairs of another."[42] However, experts have long disagreed about what types of intervention are illegal under international law.[43]

In 1970, the UN General Assembly set forth the *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations* (the declaration).[44] The declaration restates the prohibition against political interference as a violation of international law.[45] Further, the declaration states the duty of countries to "refrain from any *forcible* action which deprives peoples . . . their right to self-determination and freedom and independence."[46] The declaration also sets out a duty of states to "refrain from organizing, instigating, assisting, or participating in acts of civil strife when the acts . . . involve a threat or use of force."[47] Regarding the principle of non-intervention, the declaration states that "armed intervention and all other forms of interference . . . against the personality of the state or against its political . . . [elements] are in violation of international law."[48]

Though certain interventions may be violations of international law, it does not follow that all illegal interventions allow a state to respond in self-defense. This paper's background section mentions three terms key to determining under what conditions a state, or group of states, may exercise legal uses of force—armed attack, aggression, and use of force. While all three terms are contained within the UN Charter, there is no consensus on how they interact.[49] Aggression, the term utilized in Security Council determinations under Article 39, is not directly applicable to this paper's self-defense analysis and is used only where past proceedings have yielded insight into scenarios that may amount to a use of force or armed attack.

B. Going from International Law Violation to Armed Attack

There are at least two schools of thought regarding when an illegal use of force rises to an armed attack.[50] Under the rule adopted by the majority of the International Court of Justice (ICJ) in its judgment of the *Nicaragua* case, the term armed attack is reserved for only those "most grave" uses of force.[51] The U.S., however, rejects this gravity threshold, asserting that any use of force can qualify as an armed attack.[52] Regardless of the rule used, however, incursions into a nation's political independence under ostensibly peaceful circumstances, while perhaps coercive in nature, are seldom broadly accepted as uses of force.[53]

IV. The Effects-Based Test for the Use of Force in Cyber Operations

Cyber operations provide a new challenge to determining what constitutes a use of force. As identified in the *DoD Law of War Manual*, international law regarding cyber operations is not well-settled and will continue to develop over time.[54] During a 2017 hearing of the Senate Armed Services Committee, Senator John McCain made clear that the U.S. must have a policy addressing what constitutes "an act of war or aggression in cyberspace that would merit a military response, be it by cyber or other means."[55] Until now, the U.S. has generally applied the use of force concept to cyber operations as an effects-based test.[56]

The effects-based test focuses on activities that cause "direct physical injury and property damage."[57] For the most part, examples given previously by U.S. officials of cyber operations effects that constitute uses of force are very clear-cut, such as triggering a nuclear meltdown, causing airplanes to crash, and disrupting dam operations to flood cities.[58] Such clear examples of uses of force are helpful in establishing the premise that the U.S. considers that cyber operations may sometimes rise to a use of force, but their utility abates when considering more nuanced uses of force.

This is not to say that the DoD's use of force analysis of cyber operations is limited to those clearly articulated examples. By drawing from a 1999 DoD Office of General Counsel (OGC) assessment, the DoD recognizes that certain cyber operations may not have a "clear kinetic parallel" and that factors other than the effects of the cyber operation may be relevant to a use of force determination.[59] For illustrative purposes, the DoD provides the example of a cyber operation that cripples a military logistics system.[60] In that example, it is difficult to point to the direct physical injury and property damage caused by the attack. Instead, the use of force is determined by the resulting effect on national security through the degradation of military readiness and sustainability of operations.[61] Thus, while the U.S. clearly employs an effects-based test, the differences in the applicability of the test to direct versus indirect consequences of cyber operations reflect the current ambiguity in international law and policy regarding when cyber operations may be considered armed attacks.[62]

In the context of cyber operations, there should be a fundamental distinction between what might be termed hacking for position and hacking to undermine the game itself.

V. Updating the Use of Force Paradigm

One theme central to the practice of law, at least in common law nations, is the idea that old law (drafters' intent, previous legal decisions, and practice) ought to weigh heavily in the consideration of novel legal issues.[63] As such, lawyers rightly draw upon historical ideas regarding uses of force, armed attack, and aggression when contemplating emerging cyber operations. However, these techniques may prove inadequate or counterintuitive in the face of a revolution in the methods and means of warfare.

A. Not All Political Interference is Equal

Intervention in the political process by nations in furtherance of competing national policies and ideologies can be considered a type of gamesmanship, wherein each actor uses its pieces to gain advantage on the field of play. In the context of cyber operations, there should be a fundamental distinction between what might be termed hacking for position and hacking to undermine the game itself.[64] The former belongs to a family of activities carried on by governments long prior to the advent of the Internet in attempts to spread their ideology and obtain a favorable position in world politics.[65] In the cyber realm, this could include such things as states and their agents hacking various platforms in order to gain access to emails or other materials for purposes of intelligence gathering, conducting information operations with the intelligence gained through such activities, or spreading false news.[66] Notably, activities within this family may be illegal pursuant to the internal laws of states and the international law principle of non-intervention.[67] However, illegality does not necessarily equate to a use of force or armed attack.[68] Even if accomplished through deception, as by the spreading of false news, the country in this instance has gained position by swaying public opinion.

In contrast, hacking to undermine the game itself presents a much more forceful example. A non-cyber instance of this concept consists of training and arming a proxy group to unseat and replace, through threat of or actual violence, the existing government.[69] In the cyber realm, this example is more like targeting voter registration and election systems in order to actually change the votes already cast or even add non-existent voters that could then be exploited by a complementary covert human element.[70] In contrast to activities that influence the citizenry, the foreign power has replaced the choice of the voting public with a candidate of its own, thereby depriving the population of meaningful self-determination.

Both hacking for position and hacking to undermine the game lie somewhere in a spectrum of interference that includes all activities that qualify as interventions, with smaller subsets of possible uses of force inclusive of, but not limited to, coercion and armed attack.[71]

B. Alternate Views on Force

1. Force as Physical Violence Limiting the Right of Self-Defense. In 1989, Judge Abraham Sofaer expressed the U.S.' position on armed attack as part of an international law lecture at The Judge Advocate General's School in Charlottesville, Virginia.[72] Judge Sofaer was then-legal advisor for the U.S. Department of State.[73] Using essentially the same language later contained in the *DoD Law of War Manual*,[74] Judge Sofaer said, "The United States has long assumed that the inherent right of self-defense

potentially applies against any illegal use of force . . . ."[75] Two sentences prior to making that statement, however, Judge Sofaer says, "General Assembly interpretive declarations make clear that 'force' means physical violence, not other forms of coercion."[76] This interpretation limits the potential activities that might constitute a use of force to those involving physical violence.[77] Although Judge Sofaer's statement accurately states a longstanding U.S. position, it is interesting that the *DoD Law of War Manual*, contemplating both kinetic and non-kinetic examples, does not contain the same restrictive language as to the definition of force.[78]

2. Getting to Armed Attack Without Physical Violence. There is at least modest support for a view of force that includes "intermediate," political, and economic coercion as potential uses of force that could invoke the right of self-defense.[79] The Report of the Special Committee on Friendly Relations, prepared during preparation of UN General Assembly Resolution 2625, made it clear that there was significant debate over whether or not to define force in the resolution.[80] It is also clear that, in the end, there was no decision as to what should or should not be included in a definition of force.[81] Rather, the report states, "[t]here was no agreement whether the duty to refrain from economic, political, or any other form of pressure against the political independence . . ." of a nation should be included in the definition of force.[82]

Although the debate is helpful in establishing the long-running ambiguity in the concepts of force and armed attack in the law of armed conflict, it is unlikely that economic and political coercion will be accepted as uses of force in the near future.[83] The use of force may be viewed as equal to armed attack, as in the U.S. view, or constitute a lesser act. Either way, the winning interpretation controlling resort to self-defense right now is that armed attack must involve some level of physical violence.[84] National security law expert Matthew Waxman points out the trouble with this interpretation, writing that "[a] significant problem with [requiring violent consequences] is that in a world of heavy economic, political, military, and social dependence on information systems, the 'non-violent' harms of cyber-attacks could easily dwarf the 'violent' ones."[85] Similarly, the National Research Council's report on *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* states "Actions that significantly interfere with the functionality of [the information technology] infrastructure can reasonably be regarded as uses of force, whether or not they cause immediate physical damage."[86]

As the previous quotes suggest, there is no need to adopt the minority view that coercions are uses of force in order to address the utility of expanding armed attack to include uses of force that do not have a physical violence component. Instead, the only requirement is that there be agreement that a sovereign may be required to exercise self-defense against an attack on the self-determination right (and, therefore, political independence) of the population it governs regardless of the attack's form. Concentrating on the scale and effects of destructive cyber operations instead of relying merely on the means of delivery already stretches physical violence outside of logical limits.[87] Rather than continuing to finesse the armed attack standard into greater feats of contortion, the legally responsible course of action is to admit that the world has indeed changed and that physical violence is no longer a condition precedent to armed attack and the right of self-defense.

3. Textual Troubles with Limiting Force to Physical Violence under the UN Charter Other considerations are immediately apparent when attempting to reconcile the interplay between Articles 51 and 2(4) of the UN Charter. As previously mentioned, Article 51 explicitly states that the Charter does not limit a state's right of self-defense in response to an armed attack.[88] If the reader interprets armed attack to be limited to acts involving kinetic violence, and also reads Article 51 to limit a state's right of self-defense to only those instances of armed attack, then reading Article 2(4) use of force as anything other than armed attack means that a state could be subjected to an illegal use of force without having a corollary right to self-defense.[89]

Limiting the definition of use of force to only physically violent armed attacks not only potentially precludes self-defense, as discussed above, but also presumably precludes any action by the UN Security Council. This interpretation, however, cannot be true, as it is in conflict with Article 39, which gives the Security Council discretion to determine whether diplomatic, economic, or military measures are required when responding to an actual or threatened breach of the peace or act of aggression—actions which presumably would constitute uses of force.[90] If a threatened breach of the peace, for example, is not a use of force, then the untenable result would be that the UN Charter allows the Security Council to make war without a preceding threat or use of force from some party.

C. Self-Defense Against Cyber Operations Targeting Political Independence

1. Recent DoD Guidance On Cyber Operations. The DoD General Counsel (GC) recently released a memorandum addressing several issues regarding the DoD's use of cyber capabilities.[91] Among those issues discussed, the GC states that the Article 2(4) prohibition on use of force applies to "cyber actions that generate effects that would equate to a use of force or armed attack if caused by traditional means."[92] This point generally reflects what is current policy in the *DoD Law of War Manual*.[93] Second, the GC recognizes that coercive activities short of uses of force, including those affecting political independence, are violations of international law.[94] However, the GC is silent on whether activities affecting political independence can rise to a use of force.[95]

The traditional U.S. view of use of force has arguably served it well. As adversaries continue to close the technological gap between U.S. cyber capabilities and their own, however, the United States may out of national interest re-examine its view of force as physical violence in order to create an option of countering asymmetrical cyber threats through traditional kinetic means of warfare.

An interpretation limiting uses of force and armed attack to acts of physical violence must be rejected in applying *jus ad bellum* concepts to cyber operations against political independence.[96] In effect, using a cyber operation to trigger a dam to flood a town is an armed attack the same as if the actor had dropped a bomb. Likewise, the hostile take-

over of another country's government by cyber operation should be treated the same as if an armed force had taken the capital.

2. Drawing a Line Between Mere Interference and a Use of Force. Crucial to maintaining peace, though, is ensuring that there are legally defensible constraints preventing a country from claiming every interference is a use of force or armed attack. The current effects-based test provides a useable framework in setting such constraints. In the context of political independence, however, it is a fallacy to try to compare the effects of a cyber operation with the effects of kinetic weapons as a measure of whether an armed attack[97] has occurred.

At the root level, decision makers are using the test to determine whether the gravity of the effects caused by the cyber operation rise to the level of an armed attack.[98] Therefore, when making a use of force calculation involving political independence, decision makers must consider the gravity of actual or potential[99] effects on a country's political independence without regard to the kinetic or non-kinetic nature of those effects.[100]

Next, it is crucial that leaders differentiate interventions solely based upon peacefully influencing a population from those operations that undermine the political process.[101] On the spectrum of interference, the more an operation focuses on changing the mind of the electorate through peaceful influence, the less support available to proclaim it a use of force. Again, this is not to say that such activities are not illegal under a country's laws or in international law. Nor is it to say that countries cannot respond in a manner not amounting to a use of force against such activities.[102] Rather, the distinction is whether an operation invites a military response under the UN Charter or customary international law.[103]

Under this test, the Patriumland parliament could make a colorable argument that the hypothetical coup constituted an armed attack and therefore invited military response as an option. It is hard to think of something more crucial to the political independence of a functioning democracy than the ability of its citizens to determine their leaders. Given that the cyber operation targeted that political independence through the selection of Patriumland's most visible leader, the president, the gravity of the operation's effect is huge. Likewise, the attacking country achieved its objective, not by swaying the hearts and minds of the population through propaganda, but rather by undermining the legitimacy of the voting process.

VI. Conclusion

Cyber operations interfering with a sovereign state's political process are a hot topic in today's news and will likely continue to be such in future political contests.[104] As the risk to the actual or perceived legitimacy of the political process increases, the more likely it is that government officials will attempt to equate such cyber operations as uses of force and armed attacks.[105] The U.S. government should adopt a test for cyber operations against political independence that allows the branches of government to articulate the conditions upon which a use of force has occurred with a single voice.[106]

When considering self-defense in response to interference with political independence, leaders should consider physical violence as a factor rather than a prerequisite and focus instead on the gravity of the effect. However, those same leaders must also be careful to refrain from labeling historically equivalent non-force acts of influencing the opinions and ideologies of population, though potentially illegal, as uses of force.

Weapons will continue to evolve as long as there are humans to make them. For the purposes of armed attack, it matters not whether a weapon fires a lead bullet or lines of code. International law on armed attack and the use of force will remain relevant in a changing world by recognizing the validity of self-defense against non-kinetic threats to political independence and by integrating concepts of force that account for the effects of those threats.[107] **TAL**

Major Kinslow is presently assigned as the Deputy Staff Judge Advocate, 311th Signal Command, Honolulu, Hawaii.

Notes

1. *Transcript of Foreign Cyber Threats to the United States: Hearing to Receive Testimony Before S. Comm. on Armed Services 115th Congress* at 4 (2017) [hereinafter *Hearing*].

2. *See generally Hearing, supra* note 1. *See generally* Press Release, Dir. of Nat'l Intelligence, Joint Statement from the Dep't of Homeland Sec. & and Office of the Dir. of Nat'l Intelligence on Election Sec. (Oct. 07, 2016) [hereinafter DNI Press Release], https://www.odni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement.

3. *Id.*

4. *See generally Hearing, supra* note 1.

5. DNI Press Release, *supra* note 2.

6. *See generally* U.S. Dep't of Def., DoD Law of War Manual (May 2016) [hereinafter LoW Manual].

7. U.N. Charter Preamble.

8. U.N. Charter art. 2, ¶ 3.

9. U.N. Charter art. 2, ¶ 4.

10. Certainly the other requirements, such as that the act be that of a state, within the clause are important but are not within the scope of this paper.

11. *See generally* U.N. Charter art. 2(4).

12. *See generally* U.N. Charter. *See also* 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, 427 (2011).

13. *See generally* U.N. Charter.

14. *See generally* U.N. Charter.

15. U.N. Charter arts. 39, 42.

16. *Id.*

17. Permanent members of the United Nations Security Council include the United States, China, Russia, Great Britain, and France. U.N. Charter art. 23.

18. *Id.* art. 27, ¶ 3.

19. *Id.* art. 51.

20. *Id.*

21. *Id.*

22. *See generally* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 101-04 (June 27) [hereinafter ICJ Judgment]; *See also* LoW Manual, *supra* note 5, at 1.11.5.2 n.230 (May 2016).

23. Tallinn Manual on the International Law Applicable to Cyber Warfare 45 (Michael N. Schmitt ed. 2013) [hereinafter Tallinn].

24. *Id.* at 45

25. *Id.* at 47.

26. LoW Manual, *supra* note 6, para. 1.11.5.1 n.229.

27. Ian Brownlie, International Law and the Use of Force by States, 367 (1963).

28. http://avalon.law.yale.edu/19th_century/br-1842d.asp.

29. LoW Manual, *supra* note 6, at 1.11.5.

30. *Id.* para. 1.11.5.

31. *Id.* para. 16.1.2.

32. *Id.* para. 16.1.2.1.

33. *Id.* para. 16.1.2.2.

34. *Id.*

35. LoW Manual, *supra* note 6, at para. 16.1.2.2.

36. *Id.* para. 16.2.1.

37. Convention on Rights and Duties of States art. 3, Dec. 26,1933, 49 Stat. 3097, 165 L.N.T.S. 19.

38. Lori Fisler Damrosch, *Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs*, 83 Am. J. Int'l L. 1, 48 (1989).

39. *Id.* at 37.

40. Since this paper focuses on political independence as related to a democratic system of government, it is unnecessary to explore the philosophical debate over what interventions against an autocratic government for the ostensible benefit of the native population are illegal uses of force targeting political independence.

41. Damrosch, *supra* note 38, at 37.

42. Convention on Rights and Duties of States art. 8, Dec. 26, 1933, 49 Stat. 3097, 165 L.N.T.S. 19.

43. *Summary Records of the 56th Meeting*, [1950] 2 Y.B. Int'l L. Comm'n 159-62, U.N. Doc. A/CN.4/SER.A/1950.

44. G.A. Res. 2625, Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations (Oct. 24, 1970) [hereinafter G.A. Res. 2625].

45. *Id.*

46. *Id.* (emphasis added).

47. *Id.*

48. G.A. Res. 2625, *supra* note 44.

49. G.A. Res. 2131 (XX), Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty (Dec. 21, 1965) [hereinafter G.A. Res. 2131].

50. Tallinn, *supra* note 23, at 47.

51. Tallinn, *supra* note 23, at 47. *See ICJ Judgment*, *supra* note 22, at 191.

52. Tallinn, *supra* note 23, at 47. *See* LoW Manual, *supra* note 6, at para. 16.3.3.1.

53. Tallinn, *supra* note 23, at 46. *See also* Waxman, *supra* note 12, at 428-30.

54. LoW Manual, *supra* note 6, at para. 16.1.

55. *Hearing*, *supra* note 1, at 6 (statement of Sen. John McCain, Chairman, S. Comm. on Armed Services); *See also Hearing*, *supra* note 1, at 55-56 (statement of Sen. Debra Fischer, Member, S. Comm. on Armed Services.

56. LoW Manual, *supra* note 6, at para. 16.3.1. *See also* Waxman, *supra* note 12, at 434-37.

57. LoW Manual, *supra* note 6, at para. 16.2.1 n.9.

58. *Id.* para. 16.3.1.

59. *Id.* para. 16.2.2.

60. *Id.* para. 16.3.1. *See also* LoW Manual, *supra* note 6, para. 16.3.1 n.21, citing Dep't of Def., Office of the Gen. Counsel, *An Assessment of International Legal Issues in Information Operations* (2nd ed., Nov. 1999), *reprinted in* 76 U.S. Naval War College Int'l Law Studies 459, 483 (2002).

61. LoW Manual, *supra* note 6, para. 16.3.1.

62. *See* Waxman, *supra* note 12, at 434-35, 437, 448-49.

63. *See Precedent*, Black's Law Dictionary (9th ed. 2009).

64. *See generally Hearing*, *supra* note 1, at 39 (statement of James Clapper, Dir. of Nat'l Intelligence).

65. Damrosch, *supra* note 38, at 2-5 (1989). *See also Hearing*, *supra* note 1, at 39 (statement of James Clapper, Dir. of Nat'l Intelligence).

66. LoW Manual, *supra* note 6, at para. 5.26; Tallinn, *supra* note 23, at 46; *see also Hearing*, *supra* note 1, at 39 (statement of James Clapper, Dir. Of Nat'l Intelligence).

67. Memorandum from the General Counsel of the DoD to Commanders of the Combatant Commands et al., subject: International Law Framework for Employing Cyber Capabilities in Military Operations (Jan. 19, 2017) [hereinafter GC Memorandum].

68. *Id.*

69. *See* G.A. Res. 2625, *supra* note 44. *See also* G.A. Res. 2131, *supra* note 49.

70. *See generally Hearing*, *supra* note 1 (statement of Sen. John McCain, Chariman, S. Comm. on Armed Services).

71. *See* ICJ Judgment, *supra* note 22, at 205.

72. Judge Abraham Sofaer, *The Sixth Annual Waldemar A. Solf Lecture in International Law: Terrorism, the Law, and the National Defense*, 126 Mil. L. Rev. 89, 93 (1989). LoW Manual, *supra* note 6, at 1.11.5.2 n.230.

73. *Id.* at 8.

74. LoW Manual, *supra* note 6, para. 16.3.3.1.

75. Sofaer, *supra* note 72, at 93.

76. *Id.* at 92–93. *See also* Waxman, *supra* note 12, at 421, 427.

77. Notably, the U.S. position espoused by Judge Sofaer, while limiting uses of force to acts of physical violence, broadens armed attack to "include forms of aggression historically regarded as justifying resort to defensive measures." Abraham Sofaer, *International Law and the Use of Force*, 82 Am. Soc'y of Int'l L. Proceedings 420, 422." Those forms of aggression include "both direct and indirect complicity in all forms of violence, not just conventional hostilities." *Id.*

78. *See generally* LoW Manual, *supra* note 6, para. 16.2.2.

79. Comment, *The Use of Nonviolent Coercion: A Study in Legality Under Article 2(4) of the Charter of the United Nations*, 122 U. Pa. L. Rev. 983, 987-88 (1974). Examples of intermediate coercion given in the Comment include ideological, such as hostile propaganda, and indirect, including fomenting of civil strife. *Id.* at 990. Of note, to coerce, as defined by Merriam-Webster, means to achieve by force or threat. Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/coerce (last visited Mar. 17, 2017). Likewise, the definition of force does not require physical violence. Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/force (last visited Mar. 17, 2017); *See also* Waxman, *supra* note 12, at 449; *See also* U.N. CAOR Special Comm. on Friendly Relations, U.N. Doc. A/AC.125/SR.100 to 114 (1970); Rep. of the Special Comm. on Friendly Relations and Cooperation Among States, U.N. GAOR, 24th Sess., Supp. No. 19, at 12, U.N. Doc. A/7619 (1969).

80. Rep. of the Special Comm. on Friendly Relations and Cooperation Among States, U.N. GAOR, 24th Sess., Supp. No. 19, at 15, 20, 32-33 U.N. Doc. A/7619 (1969).

81. *Id.* at 15.

82. *Id.*

83. Tallinn, *supra* note 23, at 46.

84. Waxman, *supra* note 12, at 427-28.

85. *Id.* at 436.

86. Comm. on Offensive Info. Warfare, Nat'l Research Council, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 253-254 (2009) [hereinafter NRC Committee Report].

87. Scale and effects is the terminology used in the Tallinn manual, taken from the *Nicaragua* court, to determine when a cyber operation rises to an armed attack. *See* Tallinn, *supra* note 23, at 54

88. U.N. Charter art. 51.

89. Comment, *supra* note 79, at 987-95; *See generally* U.N. Charter art. 39.

90. U.N. Charter art. 39. *See generally* U.N. Charter.

91. GC Memorandum, *supra* note 67.

92. *Id.*

93. LoW Manual, *supra* note 6, para. 16.3.1, 16.3.3.1.

94. GC Memorandum, *supra* note 67.

95. *Id.*

96. *See* Harold Hongju Koh, Legal Adviser, Dep't of St., *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference* (Sept. 18, 2012), *reprinted in* 54 HARVARD INT'L L. J. ONLINE 7 (Dec. 2012).

97. Admittedly, the advent of cyber operations that use force against political independence stretches the term armed attack beyond its logical meaning. In the future, perhaps use of force will supplant armed attack in common usage when describing legitimate use of self-defense.

98. Tallinn, *supra* note 23, at 55. *See also* ICJ Judgment, *supra* note 22, at 195.

99. Potential is not to be mistaken here as anticipatory self-defense or as preemptive strikes under the so-called "Bush Doctrine." See Robert Jervis, *Understanding the Bush Doctrine*, Pol. Sci. Q. 365 (2003) for a discussion of the Bush Doctrine.

100. *See generally* LoW Manual, *supra* note 6, at para. 16.2.2.

101. This proposed factor examines means and methods and answers the "how" after determining that the gravity of the effect otherwise qualifies it as an armed attack. It answers whether the effect was accomplished through forcible means. It is a constraint on the effects-based test that was unnecessary when making determinations based upon physical destruction. Effects that are attributed to a change, absent coercion, in people's hearts and minds do not allow a legitimate military response.

102. LoW Manual, *supra* note 6, at para. 16.3.3.3. Examples include retorsion and countermeasures; *Id.* para. 16.3.3.3 n.33; *see also* http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/.

103. Tallinn, *supra* note 23, at 48-51.

104. *See* Zephyr Teachout, *Extraterritorial Electioneering and the Globalization of American Elections*, 27 Berkeley J. Int'l L. 162, 164 (2009).

105. *See generally Hearing*, *supra* note 1.

106. *Id.*

107. *See generally* Waxman, *supra* note 12, at 425.

Members of the 1st Security Force Assistance Bridgade salute during the SFAB's Activation Ceremony hosted at the National Infantry Museum in Fort Benning, Georgia, in February (Credit: U.S. Army photo by Patrick A. Albright).