A Better Defense

Examining the United States’ New Norms-Based Approach to Cyber Deterrence

Catherine Lotrionte

Since 2010, states have sought further methods for deterring adversarial actions through the Internet and recognized the need to develop forms of cyber deterrence as a key consideration in the pursuit of national and international security. In 2010, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) recommended that any further dialogue among states and other actors on norms pertaining to state use of Information and Communication Technologies (ICTs) to reduce collective risk and protect critical national and international infrastructure include discussions on the use of ICTs in conflict.¹

This article examines how the United States has worked to develop cyber deterrence in its more recent efforts by relying on a normative approach to establish “rules of the road” for conflict in cyberspace. It argues that the U.S. norms-based approach, in conjunction with U.S. military power, can reinforce general deterrence in cyberspace, increasing global stability. The article probes links between norms, international law, and deterrence policies, identifying conditions that may increase the potential utility of a strategic norms-based approach for calculations of military-security

Catherine Lotrionte is Director of the Institute for Law, Science, & Global Security and a Visiting Assistant Professor of Government and Foreign Service at Georgetown University. Dr. Lotrionte has served as Counsel to the President’s Foreign Intelligence Advisory Board at the White House and as Assistant General Counsel at the Central Intelligence Agency. She is the Director and Founder of the Cyber Project at Georgetown University and a Life Member of the Council on Foreign Relations.
policy in the cyber domain. It argues that by embedding cyber deterrence practice in a set of norms, the deterrence strategy will be more likely to stabilize and restrain self-help behavior of states in the cyber domain. In other words, international norms can serve as a structure to increase the chances of deterrence success.

The article notes the potential limitations of cyber deterrence as examined by many others, but maintains that a synergy exists between recent developments in international engagement on cyber norms and the academic literatures, pointing to new lines of norms-based research in constructivism that can aid in strengthening the potential for cyber deterrence for the future. The basic proposition of the article is that understanding norms, how and when they develop, and their potential to evolve into binding international law, is essential to the effectiveness of a cyber deterrence policy. Drawing on the work of Lawrence Freedman, the article illustrates how a norms-based approach, rather than an interest-based approach, better reflects how deterrence works in practice, "through actors internalizing a sense of appropriate limits on their actions." In sum, cyber weapons alone will not guarantee deterrence. If indeed cyber weapons come to be viewed as deterrent weapons it is not only because of the nature of the technology, but also through a normative context of social construction based on the interest and identity of states.

**Deterrence in a Post-Cold War Era.** As recent international events such as Estonia (2007), Georgia (2008), and Stuxnet (2010) created elevated awareness and security concerns, scholars and policymakers have turned their attention to the "cyber" issue focusing on whether deterrence theory can work in the cyber domain. Although the traditional notions of deterrence theory based on military strength have yet to mature in cyberspace, the United States has recently begun to develop a new strand of cyber strategy and policy—agreement on international norms and legal rules for cyber conflict—that I argue could deliver a positive deterrent effect. Indeed, the United States' recent policies reflect a recognition that a normative approach could indeed provide the necessary deterrent effect with regard to certain uses of cyberspace during conflict.

Some have argued that cyber deterrence as a U.S. strategic option is so discredited that it should be discarded completely. Recent scholarship has highlighted a number of challenges for cyber deterrence, illustrating the difficulty of deterrence’s translation into cyberspace and arguing, "concepts of deterrence and war may simply lack the logical foundations that they have in the nuclear and conventional realms."
Some of the barriers to cyber deterrence that have been analyzed include: limits of attribution of the adversary, difficulty in holding the adversary’s assets at risk, limits to an ability to continue an attack, involvement of non-state actors, and lack of a counterforce option. In short, some analysts have argued, the fundamental nature of the cyber domain is different than the physical domain and requires adopting new rules for state conduct and policy.

In 2009, perhaps to signal to opponents the United States’ seriousness in developing cyber capabilities for conflict, the United States established its first cyber command and has since developed significant offensive cyber capabilities. In July 2011, the then-vice chairman of the joint Chiefs of Staff General James Cartwright, spoke further about the need to develop cyber deterrence through both punitive and denial mechanisms. As Cartwright noted, “There is no penalty to attacking us now. We have to figure out how to change that.” Recently, in seeming recognition that military action in cyberspace to punish or deny using military resources may not be the best approach to deterring adversaries, a new norms-based approach to deterrence has begun to emerge in U.S. policy discussions.

In summarizing some of the options available to bolster U.S. cyber deterrence efforts, James Lewis has drawn attention to a normative component of cyber deterrence strategy:

Better defenses could be reinforced by multilateral understandings on acceptable behavior in cyberspace—explicit norms and obligations... Just as nations feel a degree of constraint from norms and agreements on non-proliferation, establishing explicit international norms for behavior in cyberspace would affect political decisions on the potential risk and cost of cyber attack. A norms-based approach to deterrence—as opposed to a strictly interests-based approach—is one that reinforces "certain values to the point where it is well understood that they must not be violated.” While this approach provides hope for developing effective cyber deterrence it will require the exercise of many elements of foreign policy, rather than the use or threatened use of military force alone.

The next section describes the recent policies announced by the United States supporting international norms in cyberspace.

The Role of the United States.

In May 2011 the United States released International Strategy for Cyberspace, its first policy document promoting international norms in the context of “applying the expectations of peaceful and just interstate conduct to cyberspace” in order to effect “stability,” as exists in “other spheres of international relations.” The document recognized that "adherence to such norms brings predictability to state conduct, helping prevent the misunderstandings that could lead to conflict.” During the same year, the Department of Defense’s Strategy for Operating in Cyberspace described how the department would work with international partners “to encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuade and deter malicious actors, and reserve the right to defend these vital national...
assets as necessary and appropriate." These policies focus on regulative norms concerned with preventing inter-state conflict, or at least shaping and limiting the use of cyber attacks in cyber conflict. As the United States promulgated its own domestic norms related to these international norms, the norms were being socialized to other states and the global cybersecurity agenda at the UN. The socialization of these norms is illustrated in states’ agreeing to the 2013 GGE report. At the UN, for the first time, fifteen states, including Russia and China, agreed that the UN Charter principles and international law, in general, applies in the cyber domain. The report also upheld the principle of state responsibility for curbing or halting cyber attacks originating in their territories.

Based on pre-existing principles of international law, specifically *jus ad bellum*, the laws related to the recourse to the use of force, and *jus in bello*, laws related to armed conflict, the United States has campaigned for international agreement on cyber norms. To date, the United States has succeeded in persuading at least fifteen states to embrace the norms of the UN Charter and state responsibility in the context of cyberspace. As a norm entrepreneur, the United States has framed the issues in a way that challenges the appropriateness of what is generally accepted today in cyber conflict. During this stage of “norm emergence,” attention was called to the issue by the United States and like-minded states, and support was built. This began the socialization process of the norm life cycle. This acceptance was possible in part because of the pre-existence of similar humanitarian issues related to conflict. As constructivist theory contends, “mutually reinforcing and consistent norms appear to strength one another.”

Although the GGE process has been an important step in the right direction, with only fifteen states in agreement, it lacks widespread international support. Only when a “critical mass” of states agree to a norm will the norm reach a “tipping point,” after which the norm gains widespread acceptance through a “cascading” effect. Although it is not possible to predict exactly how many states are needed to “tip” the process, international law suggests that the “tipping” would occur once a majority of states in the international system adopt the norm. For example, in the case of the norm of non-use of force, in the intervening years between the League of Nations in 1919, which had no mention of the norm of non-use of force, and the UN Charter in 1945, the norm achieved widespread support. It was considered so unproblematic by 1945 that at the negotiations of the UN Charter, no state felt the need to provide a public defense of Article 2(4) of the Charter. The UN Charter went
into force in 1945 with about 60 states as signatories.

Positive signs exist for further engagement on cyber issues. For example, there are signs that the United States is willing to engage with the Russian Federation on proposals to limit the military use of cyberspace, thereby reversing the trend of recent years. In 2013, General Martin Dempsey, at a public forum discussing cyber threats, explained that the Chinese “did not believe that hacking American systems violated any rules, since no rules existed.” He noted that American and Chinese officials had plans to meet to discuss ways “to establish some rules of the road” with respect to cyberattacks against U.S. companies to steal intelligence property. In July 2011, an Organization for Security and Cooperation in Europe (OSCE) resolution to share information on cyber deployments during military conflicts was co-sponsored by the United States, Russia, and other nations.

Most recently in June 2013, Russia and the United States agreed to a hotline for real-time communications during a cyber-crisis, enabling both states to avoid misunderstandings and preventing potential escalation. This is an indication of the emergence of a set of agreements between the two states to reduce conflict by contacting each other if there is a cyber incident instead of resorting to self-defense first. The United States has also conducted war games to figure out just how these rules would apply if it had to respond to a cyber attack against its critical infrastructure, and has recently updated its classified military rules of engagement in cyberspace for the first time in seven years.

Such instances of cooperative efforts can act as a mechanism for the institutionalization of the norms across states through iterated behavior and habit; frequent interactions among individuals involving joint work can ultimately create predictability, stability, and habits of trust. Expanding these efforts through informal, non-obligatory intergovernmental cooperation, confidence building measures of transparency, and the creation of internationally recognized red lines would further increase international support.

Finding Norms for Cyberspace.

During the Cold War, the Soviet Union and United States were able to establish both formal and informal arrangements to minimize the potential for catastrophic war and escalation. Today, the United States and other states have an opportunity to reach a consensus on the appropriate boundaries for state activities in cyberspace in order to avoid widespread, potentially devastating, damage in cyberspace. The U.S. efforts seeking agreement on specific norms related to international law and the use of force in the cyber domain may prove the most fruitful for international agreement. While a “no-first use” norm, like that which emerged during the Cold War, is unlikely to develop for the cyber domain, a norm of “acceptable use” could emerge, illuminating the “red lines” of cyber operations. States could agree to certain acceptable targets in cyberspace during conflict. There is international humanitarian law on the issue of legitimate targets during conflict, especially the long standing prin-
ciples of *jus in bello*, which requires civilian populations to be protected during conflict and that gains of a military action need to be proportionate by not causing unnecessary harm or suffering. Extending these principles to the context of cyber conflict could be instrumental in developing an understanding that during a conflict in cyberspace military installations would be legitimate targets for cyber attacks, but financial institutions would not be legitimate targets given the uncertainties or unacceptable collateral damage to civilian populations. Targets such as banks, global positioning systems, and other infrastructure used for both military and civilian purposes could, under the current interpretation of the law, be legitimate targets in cyber conflict unless states were to agree otherwise.

In exploring additional options for regulating state behavior in cyber, the scenario of intrusions against industrial control systems illustrates the need for more clarity. Numerous critical installations of states such as power plants, nuclear plants, dams, water treatment and distribution systems, oil refineries, banking systems, hospital systems, and air traffic control systems rely on supervisory control and data acquisition systems, and distributed control systems. Some have proposed that it would be beneficial to prohibit cyber intrusions against industrial control targets, such that any cyber operation against such targets “would be interpreted as the prelude to an attack,” reasoning that an intrusion against such a target could only be useful as preparation for a future attack since there is no “intelligence value to hacking an industrial control system.”36

This approach would be helpful in the case of a state considering the use of anticipatory self-defense under circumstances when it would be difficult to identify with certainty the purpose behind a particular cyber operation. In the context of intrusions into industrial control systems, for instance, it would be challenging to distinguish a cyber intrusion of a state’s air defense that is meant as an *intelligence collection operation*—theft of information—from the same technical intrusion meant to identify vulnerabilities in anticipation of a *cyber attack* with physical, destructive results. Under the current understandings of the norms related to espionage versus “armed attack” under the UN Charter, an implant that is meant to support a subsequent “armed attack” would merit, and the law would allow for, a more hostile use of force response, in contrast to the discovery of a similar implant that was meant only to support espionage. This is due to the fact that under traditional understand-

**A shared understanding about** the negative ramifications for all states of such actions could be effective in constraining state behavior even without a treaty prohibiting such actions.
nings of international law, espionage does not constitute a “use of force” for purposes of the UN Charter, and certainly not an “armed attack.” Therefore, the victim of such a cyber intelligence collection operation would not have the lawful right of forcible self-defense whereas the victim of a cyber attack would, under the UN Charter, have the right of a forcible self-defense response.

This traditional understanding of the law may not be acceptable to states in the cyber context where the distinction between the cyber weapons used for intelligence collection and those used for sabotage cannot easily be made. And yet there is likely not going to be an amendment to the UN Charter to accommodate this complexity especially since state practice has indicated an unwillingness to consider intelligence collection a “use of force.” In this case, a new understanding of acceptable behavior under such circumstances would require states to reach a new agreement given the facts specific to cyber operations.

In the case of control systems, securing states’ agreement to refrain from conducting cyber attacks against such systems certainly would be useful. A shared understanding about the negative ramifications for all states of such actions could be effective in constraining state behavior even without a treaty prohibiting such actions. Indeed, there is some evidence that this may be an area that states, at least some states, would be restrained. The United States, for instance, in at least two different instances decided not to conduct cyber attacks against foreign financial networks. The Bush and Clinton admin-

istrations both refused to authorize hacking into foreign financial systems because of concerns of collateral damage and possible blowback on the United States. Yet, the question remains whether other states would agree to refrain from doing the same. A shared understanding among states that financial institutions ought not to be targets for a cyber attack would be useful especially for the United States since it already appears to refrain from such actions.

**Challenges to Application.** International law will play an important role in the normative framework for cyber deterrence as it is the international legal framework of “war” that provides the basis for cyber operations. Over the last decade, the growing concern over increased violence and the potential for state conflict in the cyber domain has led international legal scholars to assess how to accommodate an international legal framework for warfare in cyberspace, trying to bring some clarity to how international law would apply in the context of cyber conflict. In particular, the applicability of international regarding the use of force and the right of self-defense is central to any clarification of when and under what circumstances a disruptive exploit in cyberspace could be considered an armed attack, triggering a use of force in self-defense.

The most relevant international law on the issue of deterrence and the use of cyberweapons is the law relating to the use of force enshrined in the UN Charter, *jus ad bellum*, and the law applicable in armed conflict that regulates the conduct of hostilities, *jus in
bello. The UN Charter and customary law determine when cyber operations may be conducted, namely, in self-defense. While it is not necessary to fully explain the UN Charter paradigm here, it is necessary to address the issue of "use of force" and "armed attack," two of the key terms in the Charter paradigm. The Charter prohibits "the threat or use of force against the territorial integrity of political independence" of a state. Therefore, any cyber operation that amounts to a use of force is illegal. The UN Charter, however, does not allow the victim of a cyber operation that amounts to a "use of force" to respond in forcible self-defense. Such responses are limited to activities that equate to an armed attack pursuant to Article 51 of the Charter.

Based on the interpretation of these principles by the UN Charter and the International Court of Justice (ICJ), a state's ability to signal a "strike back" deterrent to a cyber operation in self-defense would be subject to a finding that the cyber operation was not only a use of force but also an armed attack. Unfortunately, neither the Charter nor the ICJ has provided specific definitions for these terms. In addition, there has yet to be a reported cyber operation between states that has been acknowledged as a use of force, let alone an armed attack. The recent Stuxnet cyber operation against the Iranian nuclear capabilities is likely to be the closest. Yet there is debate as to whether Stuxnet was a use of force or an armed attack for purposes of the UN Charter.

Recent efforts to incorporate cyber warfare in our long-standing international legal systems prohibiting the use of force and protecting civilians from the effects of war illustrate the considerable challenges and incongruities in attempting to fit cyber into the conventional armed conflict framework. Two notable efforts have been the Tallinn Manual on the International Law Applicable to Cyber Warfare (the Manual) and the International Committee of the Red Cross’s (ICRC) first major article on cyber warfare published in 2012. In the ICRC article, the ICRC disagrees with the Manual’s position on what would constitute an "attack" during armed conflict requiring physical effects. According to the majority of the experts on the Manual, "interference with functionality qualifies as damage" for purposes of determining if something was an "attack" during an armed conflict, "if restoration of functionality requires replacement of physical components." The ICRC, on the other hand, concludes that "disrupting the functioning of certain systems by interfering with their underlying computer systems can amount to damage insofar as it impairs their usefulness," and therefore, an attack would also "be understood to encompass such operations that disrupt the functioning of objects without physical damage or destruction, even if the disruption is temporary." Disagreement among the group of experts who drafted the Manual and the ICRC highlights the challenges in applying existing international law to the cyber domain.

Overcoming the Obstacles. Over centuries, in the context of the physical realm, the international legal terms of "use of force," "armed attack," and "self-defense" have come to have mean-
ing in treaties, the practice of states, and through the dispute resolution process at the UN Security Council and the International Court of Justice. Today, for such activities in cyberspace, we need new consensus about the meanings of these legal terms, how they apply in cyberspace, and the situations in which the different thresholds would be triggered based on cyber operations. It is important for states to understand what would constitute an armed attack in cyberspace that would then trigger the target state’s right of self-defense. Given that most of the malicious cyber activities that have occurred to date fall below the level of the use of force and armed attack thresholds of the UN Charter and the laws of armed conflict, uncertainty remains about the rules meant to constrain behavior that apply in the cyber domain. In order for deterrence to work and widespread agreement on cyber norms to occur, there needs to be some shared expectations between states about what is acceptable behavior and what is not acceptable behavior in the cyber domain.

In lieu of any formal international treaty defining these terms in cyber, agreeing to norms will be important to providing needed clarity for states to understand the context in which they are operating in the cyber domain. Those norms that are clear and specific, rather than ambiguous and complex, and those that have been around for a long period of time, surviving numerous challenges are more likely to be effective. Starting with those norms related to the use of force in cyberspace, where there is legal precedent, makes sense. The next step would be to come to agreement on the meaning of the terms as used in the UN Charter. For example, the United States could seek to develop a specific domestic policy articulating when Article 51 of the UN Charter would be triggered by a cyber incident, establishing a clear threshold and share it with other states in order to seek agreement.

As deterrence theorists have argued, in order for deterrence strategy to work, states must be aware of the “rules and logic of the [strategic] game” which is communicated between states and which serves not only to inform their actions but also their identities. As part of a cyber declaratory deterrence policy, U.S. statements about doctrine can influence both the likelihood and consequences of cyber attacks by helping shape global norms about reasonable and legitimate potential use of cyber weapons. To develop such norms, threats of military action alone will not suffice. Rather, the diplomatic elements of foreign policy will need to be exercised to establish and reinforce certain values to the point where it is well understood by states that they must not be violated. Clear statements by the United States would be useful in setting forth the specifics of what those values are as envisioned in cyberspace.

Conclusion. These recent events support the emergence of a U.S. national cyber strategy where cyber deterrence is pursued not solely through national security capabilities (the development of offensive cyber capabilities at U.S. Cyber Command), but also through diplomatic and normative, means.
Placing issues of cyber conflict under the auspices of the UN and the UN Charter principles makes sense. This will ultimately make the development of the norms easier for states to accept by embedding them in already existing international law and an international organization with members with conflicting identities and competing interests that plays an important role in norm innovation, cascading, institutionalization, and enforcement. Because of the lack of clarity in international law on the meaning of terms like “armed attack,” more work is required to identify exactly what the norm is and what constitutes violation as well as spelling out the procedures by which norm leaders coordinate disapproval and sanctions for norm breaking.

This article has argued that a norms-based approach, in conjunction with military cyber power, can deliver some cyber deterrence where military power alone is limited. Although the emergence of norms in cyberspace is in its early stages and it is too early to predict how these emerging norms, there are two central factors that support the potential for broader support for the norms the United States is promulgating. First, there is a tradition of international law and norms on which the cyber issues can be based that codify the principles of uses of force, self-defense, proportionality, discrimination and unnecessary suffering, principles which support the norms the United States is promoting through the GGE process. Second, the UN GGE process provides an organizational platform for the issues. With a platform like the UN, the United States and other states can act as norm entrepreneurs to bring the issue to the forefront of international public awareness.

The “rules of acceptable behavior” that cyber deterrence scholars and recent U.S. cyber strategy documents have discussed, fit into this category of “rules of the game” that can take the form of consensual bilateral or multilateral declarations of principles, or even unilateral declarations and actions. The United States presently prefers non-legally binding agreements for cyber as compared to Russia that has advocated for an international treaty. The rationale for non-legally binding agreement may be that such agreements offer decision-makers opportunities to learn about the social effects of particular sets of rules over time, amending them accordingly, typically with lower negotiation costs than entailed by the renegotiation of treaties.58 States may need time to learn about the technology and to arrive at conclusions about the kinds of behavior they prefer in the new domain of cyberspace.

Embedding the new cyber norms as stated in the GGE report in pre-

U.S. statements about doctrine can influence both the likelihood and consequences of cyber attacks by helping shape global norms about reasonable and legitimate potential use of cyber weapons.
existing and widely accepted international legal principles may alleviate the need for a separate, stand-alone treaty for cyber conflict. Indeed, given the political context for cybersecurity where mistrust and geopolitical rivalry among states exists, such informal norms may be more attractive given that it is easier involvement in the Stuxnet cyber operation against Iran’s uranium facility, the United States will likely face criticism and allegations of double standards. The United States must find a way to address these concerns and not lose momentum in the socialization of cyber conflict norms.

With a platform like the UN, the United States and other states can act as norm entrepreneurs to bring the issue to the forefront of international public awareness.

Unfortunately, the study of cyber deterrence and cyber norms is hampered by its novelty and much needed work is required to understand the processes of cyber deterrence development and normative change. Deterrence specialists have begun to pay careful attention to cyber attacks and that needs to continue. Their insights into issues related to the challenges of attribution and proportionate retaliation will be needed. The important question for international relations and legal scholars will involve understanding which norms will become legally binding international law and how, exactly, compliance with those laws comes about. It is, after all, these legal rules that will guide and determine the political actors’ behavior in the cyber domain. Understanding the mechanisms and the likelihood of compliance will be the key to the longevity of peace and stability in cyberspace.

2 Lawrence Freedman, Deterrence (Polity, 2004), p. 5.


5 Stuxnet is a computer worm discovered in June 2010 that is believed to have been created by the US and Israel to attack Iran’s nuclear facilities. "Legal Experts: Stuxnet Attack on Iran Was Illegal "Act of Force.” Wired, March 25, 2013.


13 Barnes and Gorman, "Cyberwar Plan.”


16 Lawrence Freedman, Deterrence, 4.


21 UN Report by the Group of Governmental Experts on Developments in the Field of International and Telecommunications In the Context of International Security (June 24, 2013), A/68/98, [hereinafter the UN GGE 2013 Report], http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98. The UN group consisted of fifteen nominated by the Governments of Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, the Russian Federation, the United Kingdom and the United States. The GGE was originally set up in 2002 by the UN Secretary –General to study existing and potential threats in the sphere of information security and how nations could cooperate to overcome them. During its initial years, the group was unable to make any concrete progress, failing to get agreement on specific norms. With strong US leadership, however,
the group was able to come to important consensus on some of the "rules of the road" for using force in cyberspace.

22 Martha Finnemore describes three stages of a norms life-cycle: (1) norm emergence; (2) norm cascade or broad norm acceptance; (3) norm institutionalization. See Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," International Organization, vol 52, no. 4, Autumn 1998, pp. 887-917.


24 For example, in the case of the ban on landmines, Finnemore and Sikkink argue that, "by May of 1997 [when] the number of states supporting the ban on anti-personnel mines reached 60, or approximately one third of the total states in the system. After that point, a norm cascade occurred and 124 states ratified the Ottawa Landmine treaty in December of 1997." Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," International Organization 52, No. 4 (1998), 887-917, 901

25 International law has had to grapple with this issue in the context of determining when a practice of states has risen to the level of establishing a customary international law. For a rule to be a customary international law there must be practice of states and the belief that the practice is legally obligatory. See ICJ, Continental Shelf case (Libyan Arab Jamahiriya v. Malta), Judgement, 3 June 1985, ICJ Reports 1985, pp. 29–30, § 27. ("It is of course axiomatic that the material of customary international law is to be looked for primarily in the actual practice and opinio juris of States."). The second requirement for a rule of general customary international law to come into existence is that the State practice concerned must be both extensive and representative. It does not, however, need to be universal; a "general" practice suffices. No precise number or percentage of States is required. One reason why it is impossible to put a precise figure on the extent of participation required is that the criterion is in a sense qualitative rather than quantitative. That is to say, it is not simply a question of how many States participate in the practice, but also which States. In the words of the International Court of Justice in the North Sea Continental Shelf cases, the practice must "include that of States whose interests are specially affected."


35 The US formulation of its no-first use policy was first stated by the US at a UN Special Session on Disarmament in 1978. In 1982, the Soviets declared its pledge not to resort to the first use of nuclear weapons. However, in 1993, Russia renounced the 1982 Soviet policy of no-first use. Harold A. Feiveson and Ernst Jan Hogendoorn, "No First Use of Nuclear Weapons," The Nonproliferation Review, Summer 2003, p. 2-3.

36 Lewis PAGE

37 James Lewis, Conflict and Negotiation, 53. 38 Clarke and Knake, Cyber War, 202–203.


40 UN Charter, Art. 2, para. 4.


43 UN Charter, Art. 51.
44 Military and Paramilitary Activities in and Against Nicaragua (Nicar. V. U.S.), Judgment, 1986 ICJ 14, paras. 191, 210 (June 27) (“[M]easures which do not constitute an armed attack . . . may nevertheless involve a use of force.”)

45 Roscini, at 113.


49 Id.


51 Cordula Droege, “Get off my cloud.” 27.


59 Richard Price argues that the landmine norm resonates with pre-established norms of humanitarian law, providing an advantage for the norms development. This is described in the norms literature as grafting norms, embedded norm discrimination, or nestling. Richard Price, “Reversing the Gun Sights: Transnational Civil Society Targets Land Mines,” International Organizations Vol, 52, no. 3 (1998), 613-644, 628.