William Mitchell Law Review

Volume 38 | Issue 5 Article 4

2012

Responses to the Five Questions

Jody M. Prescott

RESPONSES TO THE FIVE QUESTIONS: FIRST QUESTION

Jody M. Prescott[†]

1. TEN YEARS AFTER 9/11, WHAT IS THE MOST SIGNIFICANT LEGACY LEFT BY THE TERRORIST ATTACKS? ARE WE SAFER?

I. Introduction

From a national security and military perspective, perhaps the most significant legacy of the terrorist attacks ten years ago is not the wars that followed the attacks, nor is it the rapid evolution of military and paramilitary tactics and technology in response to dealing with a resilient and adaptive set of adversaries during the course of these wars. I suggest instead that the most important effect is the change that has occurred in the way the United States' national security and military organizations have begun to think holistically about the future use of force in complex environments. The counterinsurgency strategy that proved useful in Iraq has not achieved the same degree of success in Afghanistan, but its formulation and application mark an important milestone in the evolution of the United States' thinking about the use of different forms of influence, and about the ripple effects of both kinetic and non-kinetic actions in a theatre of operations fought amongst the people.[1] Recently, the Obama Administration has taken further steps in the implementation of such an approach with the United States' participation in the NATO campaign to assist the former rebels in Libya and the dispatch of special forces troops to assist African forces in executing the International Criminal Court's arrest warrant for Joseph Kony of the Lord's Resistance Army. Further, at the strategic level, the Department of Defense began

[†] Non-resident senior fellow, West Point Center for the Rule of Law. This article represents neither the official position of the United States Military Academy nor the United States Army. I wish to thank Major John Dehn for his invaluable assistance in reviewing this manuscript.

[1] GENERAL SIR RUPERT SMITH, THE UTILITY OF FORCE: THE ART OF WAR IN THE MODERN WORLD 269–373 (2007).

planning for possible future military actions congruent with the Mass Atrocity Response Operations concept developed collaboratively by the Carr Center for Human Rights, Harvard's Kennedy School, and the U.S. Army Peacekeeping and Stability Operations Institute.[2]

These are important examples, but where does one find the lessons learned and taken to heart, and the resulting principles that guide the thinking on how to approach future operations in these sorts of environments? Although it is ordinarily imprudent to base an analysis of an evolving national approach to working within the international security environment upon a small sample of high level policy documents, an assessment of the Obama Administration's recently released *International Strategy for Cyberspace*,[3] and the unclassified version of the Department of Defense's (hereinafter referred to as "DoD") *Strategy for Operating in Cyberspace*,[4] may in fact provide a snapshot of what the United States believes it has learned since 9/11. It also provides a snapshot of how the United States intends to apply this awareness in a crucial and complex operational area characterized by rapidly evolving technology, shadowy and amorphous actors, and uncertain legal and policy norms.

II. International Strategy for Cyberspace

Because of the way *International Strategy* is structured, analysis of it—even for the purpose of seeking to identify overarching principles—must focus in large part upon content and, therefore, tends to be descriptive. First, as to the end state the United States desires to achieve through international action, the strategy envisions:

> [A]n open, interoperable, secure, and reliable information and communications infrastructure that

[2] *See generally* SARAH SEWALL, DWIGHT RAYMOND, & SALLY CHIN, MASS ATROCITY RESPONSE OPERATIONS: A MILITARY PLANNING HANDBOOK (2010) (highlighting various attributes of the Mass Atrocity Response Operations (MARO) Project), *available at* http://www.hks.harvard.edu/cchrp/maro/pdf/MARO_Handbook_4.30.pdf.

[3] THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf[hereinafter INTERNATIONAL STRATEGY].

[4] DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf [hereinafter DOD STRATEGY].

> supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace.[5]

To achieve this goal, *International Strategy* sets out complementary diplomatic, development, and defense objectives. In terms of diplomacy, the United States intends to build consensus among states which favor "an open, interoperable, secure, and reliable cyberspace," and that will "work together and act as responsible stakeholders."[6] This consensus would be furthered through achievement of *International Strategy*'s development objective, which is to promote the building of cyber security capacity internationally, thereby strengthening global networks through the enhanced protection of different national digital infrastructures.[7]

The accomplishment of the defense objective is likely to prove the most challenging in developing consensus as to the applicable legal norms, because the use of force in cyberspace is particularly controversial. In describing the defense objective, *International Strategy* notes that the United States "will defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies. . . . [using] a range of credible response options."[8] The purpose of such actions is to, "along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate."[9] The defense objective relies heavily on dissuading malicious actors from committing unfriendly acts, and *International Strategy* phrases this aspect of the objective in positive terms, as it emphasizes the fostering of a robust cyber defense capacity both in the United States and abroad. The deterrence aspect, however, is described much more plainly. In conducting deterrence operations, the United States states that it "will ensure that the risks associated with

[5] INTERNATIONAL STRATEGY, *supra* note 3, at 8.

[6] *Id.* at 11.

[7] *Id.* at 11–12, 14–15.

[8] *Id.* at 12.

[9] *Id.*

attacking or exploiting our networks vastly outweigh the potential benefits."[10] *International Strategy* recognizes "that cyberspace activities can have effects extending beyond networks; such events may require responses in self-defense."[11] It further notes:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. . . . [A]nd we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means . . . as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.[12]

In seeking to achieve these objectives, *International Strategy* sets out three basic principles that will guide the United States in working to this end state: fundamental freedoms, privacy, and the free flow of information.[13] Fundamental freedoms are described as "the ability to seek, receive and impart information and ideas through any medium" as an internationally recognized civil liberty.[14] "Privacy" is defined in terms of a balance to be struck between individuals' expectations as to the fair use and protection of their personal data, and the need to prevent criminal activity against personal information through regulated law enforcement actions.[15] *International Strategy* defines the principle of "free flow of information" as the fostering of an information-exchange environment, which is "a level playing field that rewards innovation, entrepreneurship, and industriousness, not a venue where states arbitrarily disrupt the free flow of information to create unfair advantage."[16]

This end state will be both promoted and undergirded by the norms that result from the United States' "work with like-minded states to establish an environment of expectations . . . that ground foreign and defense policies and guide international partnerships."[17] This is important to the United States because of

[10] *Id.* at 13.
[11] *Id.*
[12] *Id.* at 14.
[13] *Id.* at 5.
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.* at 9.

the uncertainty that has developed as governments "seeking to exercise traditional national power through cyberspace" find themselves doing so without "clearly agreed-upon norms for acceptable state behavior in cyberspace."[18] In addressing this gap, the United States' position is that the "[l]ong-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace," but that the "unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them."[19] Addressing this uncertainty, therefore, will require reaching "a consensus on what constitutes acceptable behavior, and a partnership among those who view the functioning of these systems as essential to the national and collective interest."[20] The United States does not believe that reaching this consensus requires either "a reinvention of customary international law" or rendering "existing international norms obsolete," but instead sees these as a basis upon which to build consensus.[21]

Expanding upon the three basic principles that would guide the United States in its strategic approach to achieving the end state, *International Strategy* identifies the five basic principles that will undergird these norms as "Upholding Fundamental Freedoms," "Respect for Property," "Valuing Privacy," "Protection from Crime," and, perhaps most importantly for this article, the "Right of Self-Defense."[22] *International Strategy* posits that "[c]onsistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace."[23] Interestingly, *International Strategy* also identifies five emerging norms seen as essential to the proper use of cyberspace: "Global Interoperability," which is a functioning internet to which all would have access;[24] "Network Stability," which would prevent states from "arbitrarily [interfering] with internationally interconnected infrastructure;"[25] "Reliable Access," such that states would not arbitrarily interfere with individuals

[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.* at 10.
[23] *Id.*
[24] *Id.*
[25] *Id.*

accessing the internet;[26] "Multi-stakeholder Governance," meaning the inclusion of non-state actors;[27] and "Cybersecurity Due Diligence," defined as the obligations of states to protect their "information infrastructures and secure national systems from damage or misuse."[28]

Although the third section of *International Strategy*, entitled "Policy Priorities," is largely reiterative, it states with greater specificity the strategic necessity of sustaining technological innovation, protecting intellectual property, and improving the security of the high-tech supply chain to better promote efforts to combat cybercrime, to enhance multiple stakeholder governance, to protect civil liberties, and to develop agreed-upon norms of cyberspace behavior.[29] The information contained in this prioritization is helpful because it potentially sets out a checklist that United States negotiators might consult to determine if negotiating partners were, at least from the perspective of the United States, sufficiently "like-minded." Judging by the provisions of the G-8 joint declaration issued at the conclusion of the May 2011 Deauville Summit, which dealt with the internet, there is apparently great agreement among the NATO allies, Japan, and Russia on the principles and goals of internet use and governance—at least with regard to diplomacy and development.[30] Must a partner state agree on all three of the United States' objectives, or is it sufficient to find common ground on two, or perhaps just one ground, to be included in the coalition of similar thinking? This question is likely to be of great significance in determining how the United States approaches work in cyberspace with China and India.

III. DoD Strategy for Operating in Cyberspace

The unclassified version of the subsequent *DoD Strategy*, released two months after the Administration's strategy, was criticized by a number of commentators for failing to explicitly

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.* at 17–24.

[30] *See Renewed Commitment for Freedom and Democracy*, G-8 FRANCE 2011, http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html (last visited Apr. 19, 2012) (describing G-8's commitment to Internet use and governance).

explain the standards, which would guide the use of force by the United States in response to a cyber attack.[31] The U.S. Senate Committee on Armed Services quickly reminded the Secretary of Defense that DoD had agreed to provide a report to the committee by December 2010 that addressed "a number of critical questions . . . including the relationship between military operations in cyberspace and kinetic operations; . . . the rules of engagement for commanders; the definition of what would constitute an act of war in cyberspace; and what constitutes the use of force for the purpose of complying with the War Powers Act."[32] Rather than focusing on the use of force, however, *DoD Strategy* instead sets out five complementary strategic initiatives that emphasize the importance of creating a well-organized, trained, and equipped cyber force structure.[33] In essence, these initiatives all work towards two main lines of strategic effort: creating partnerships with civilian governmental agencies, private industry, allies, and other international partners and developing a national wellspring of talent and innovation to keep the United States military and industry competitive in the cyber arena.[34] *DoD Strategy* does note the use of "active cyber defense" as an operating concept, but defines it in a facially benign manner as the "synchronized, real-time capability to discover, detect, analyze and mitigate threats and vulnerabilities."[35] This definition is not completely consistent with statements made by certain U.S. officials, which indicated that this concept also entailed operations within other states' digital

[31] *See, e.g.*, Sean Lawson, *DOD's "First" Cyber Strategy is Neither First, Nor a Strategy*, FORBES.COM (Aug. 1, 2011), http://www.forbes.com/sites/seanlawson/2011/08/01/dods-first-cyber-strategy-is-neither-first-nor-a-strategy/; Jared Serbu, *DOD Strategy Aims At Deterrence*, FEDERALNEWSRADIO.COM (July 15, 2011), http://www.federalnewsradio.com/?nid=697&sid=2457989.

[32] Letter from John McCain, Ranking Member, U.S. Senate Comm. on Armed Servs., & Carl Levin, Chairman, U.S. Senate Comm. on Armed Servs., to Leon Panetta, Sec'y of Def. (July 20, 2011), *available at* http://mccain.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=40ca96ab-ec9e-4662-a360-0c1806e44f4e. The authors must have meant the War Powers Resolution, which requires that the President inform Congress within forty-eight hours if U.S. forces are engaged in combat, and that Congress authorizes continued military engagement in excess of sixty days. 50 U.S.C. §§ 1541–48 (2006); William J. Lynn, III, Deputy Sec'y of Def., Remarks on the Department of Defense Cyber Strategy, address at the National Defense University (July 14, 2011) [hereinafter Lynn Remarks].

[33] DOD STRATEGY, *supra* note 4, at 5–10.

[34] *Id.*

[35] *Id.* at 7.

infrastructure.[36] Such operations could conceivably violate long-standing legal and policy norms regarding neutrality and would raise additional questions as to the use of force threshold that would need to be met for a state to react to a cyber attack in self-defense.

To have a better idea of what the classified version of *DoD Strategy* contains regarding the use of force, it is perhaps useful to consider *DoD Strategy* in the context of the official statements made at the time of its launching. In remarks made at the formal announcement of *DoD Strategy* at the National Defense University in July 2011, Deputy Secretary of Defense William J. Lynn first noted the wide breadth of the threat spectrum, ranging from developed and responsible state actors possessing sophisticated cyber capabilities at one end, to opportunistic criminal actors and "rogue states" at the other.[37] Deputy Secretary Lynn observed that, although deterrence might have effectively discouraged major state actors from undertaking destructive cyber measures against the United States, terrorists and rogue states, which had "few or no assets to hold at risk," were not as likely to be dissuaded from conducting such operations by the same response measures.[38] Deputy Secretary Lynn provided a snapshot of the current situation in cyberspace, describing it as evidencing a temporary imbalance in capability and intent between the different possible actors.[39] Those actors with sophisticated capabilities were developing even "[m]ore destructive tools" but were not likely to use them in the near term.[40] Actors with the greatest intent to inflict harm were without such capabilities but would acquire them in time.[41]

Although he believed that in the future we are likely "to see destructive or disruptive cyber attacks that could have an impact analogous to physical hostilities," Deputy Secretary Lynn noted that "the vast majority of malicious cyber activity today does not cross this threshold."[42] Deputy Secretary Lynn's use of the word "analogous" to describe the relationship between war-like acts in

[36] Ellen Nakashima, *Pentagon Considers Preemptive Strikes as Part of Cyber-Defense Strategy*, WASH. POST Aug. 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/28/AR2010082803849_pf.html.

[37] Lynn Remarks, *supra* note 32.

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

the geophysical world and serious unfriendly acts in cyberspace suggests that, in the classified version of *DoD Strategy*, DoD has not directly incorporated international humanitarian law concepts and applications governing the use of force. Earlier statements by DoD officials had suggested that the new DoD strategy would rely on a concept of "equivalence" between geophysical world conflict and cyber action to guide its use of force in cyberspace,[43] and, on the spectrum of similarity with "identical" at one end and "completely different" on the other, equivalence might likely be closer to identity than analogy. If so,· this could have profound impacts upon the application of international humanitarian law in cyberspace.

In reemphasizing the holistic nature of *DoD Strategy*, however, Deputy Secretary Lynn pointed out that, although the United States reserved "the right, under the laws of armed conflict, to respond to serious cyber attacks with a proportional and justified military response at the time and place" of its choosing, *DoD Strategy* focused upon defensive and confidence-building measures, which would be constructed and applied through partnerships with civilian government agencies, industry, and international allies.[44] Deputy Secretary Lynn's earlier description of active cyber defense, however, suggests that the language in the classified version of *DoD Strategy* might be more aggressive than that provided to the public in the unclassified version.

IV. Possible Lessons Learned

With these issues in mind, assessment of the cyber strategies suggests nine main points that evidence the overarching principles the United States appears to have decided to apply to the use of force since 9/11.

1. *Terrorism Is a Significant Threat but Not the Organizing Theme of* International Strategy

   International Strategy is not focused upon terrorism: in reading the text, one sees that the word "terrorists" appears on only two separate pages,[45] and the words "non-state actors" occur

[43] Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J., May 31, 2011, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

[44] Lynn Remarks, supra note 32.

[45] *See* INTERNATIONAL STRATEGY, *supra* note 3, at 12, 20.

only twice in the document.[46] Cyber terrorism is instead just one aspect of an operational environment, and the strategy shows flexibility in using either law enforcement or military means, or both, to engage it. The *DoD Strategy* discusses terrorism more often, but it still is not the most significant aspect of the strategy.

2. *Holism Is Essential in a Complex World*
   Both strategies are cast in largely positive terms in creating a holistic perspective, and they emphasize the very influential civil liberties aspect of cyberspace use and the far-reaching economic significance of connectivity. The important role played by social media in the uprisings in different Arab countries in the early part of 2011 provides a credible empirical basis for concluding that this holistic approach is not just fluff and that soft power is just as real a power as military strength.[47]
3. *Networks Understand Networks*
   The holistic approaches of both strategies also show that the United States appreciates that a networked approach to dealing with a network, whether it is al Qaeda as a geophysical world threat or a threat on the Internet itself, is likely to be the most fruitful course of action in disarming it.
4. *Collective Security Organizations Remain Relevant*
   In specifically noting that certain aggressive actions in cyberspace against the United States or its allies could trigger self-defense responses pursuant to collective self-defense treaties, the United States recognizes the enduring value of formal multilateral organizations such as NATO in dealing with non-traditional threats. Formal organizations are better suited to creating standing processes to deal with emerging international threats, as NATO has done with its Cyber Defence Management Board.[48]
5. *Rule of Law Is Essential to Democracies Succeeding*
   Just as the United States has come to appreciate the complementary relationship between security and the rule of law in the geophysical operational environment of

[46] *See id.* at 13, 21.

[47] *See China Calls U.S. Culprit in Global 'Internet War,'* ABCNEWS.COM (June 3, 2011), http://abcnews.go.com/Business/wireStory?id=13750409.

[48] *NATO and Cyber Defence*, N. ATLANTIC TREATY ORG., http://www.nato.int/cps/en/natolive/topics_78170.htm (last visited Apr. 19, 2012).

Afghanistan,[49] *International Strategy* makes the same connection in cyberspace.

6. *Civilian and Military Organizations Must Cooperate to Be Most Effective*
   Given the Internet's ubiquity, *International Strategy* recognizes the important complementary relationships between civilian and military agencies in countries in terms of dealing with cyber threats. In practice, this is demonstrated by the recent memorandum of agreement between the DoD and the Department of Homeland Security setting out the terms of their cooperative efforts in cyberspace security.[50]
7. *Protecting Global Assets Requires Global Partnering*
   In terms of working internationally, *International Strategy* recognizes the need for greater global inclusiveness, not just in terms of building cyber security capacity in other countries but also in terms of setting the norms according to which that security will be executed, by expanding "this work to geographic regions currently underrepresented in the dialogue—most notably Africa and the Middle East—to further our interest in building worldwide capacity."[51]
8. *Non-State Actors Can Play an Important Role in Governance*
   Although *International Strategy* emphasizes the role of states in bringing about cyber security, it does recognize that governments and industry are not the only actors with a stake in the governance of cyberspace. It views the participation of regional organizations, civil society, and academia as being likewise important in shaping the norms by which the Internet should be governed.[52]
9. *Development of New Legal and Policy Norms Requires Consensus*
   Finally, and most importantly for purposes of this article, the United States would appear to have concluded that, if it is seeking to have a role in defining the application of international law and security policy in an area which is unsettled or which does not conform completely to existing

[49] Sebastian Rietjens et al., *Measuring the Immeasurable? The Effects-Based Approach in Comprehensive Peace Operations*, 34 INT'L J. PUB. ADMIN. 329, 332–34 (2011).

[50] Cheryl Pellerin, *DOD, DHS Join Forces to Promote Cybersecurity*, U.S. DEPARTMENT DEF. NEWS (Oct. 13, 2010), http://www.defense.gov/news/newsarticle.aspx?id=61264.

[51] INTERNATIONAL STRATEGY, *supra* note 3, at 18.

[52] *Id.* at 12.

understandings and applications, this is best done by building consensus rather than striking out on a new path unilaterally, as the Bush Administration did in the period immediately after 9/11 with regard, for example, to the treatment of detainees in a non-traditional, transnational armed conflict.[53] The cyberspace strategies place significant reliance upon coalitions of the like-minded to serve as the nuclei for developing consensus on the norms of cyber behavior expected of responsible actors. This is different than a "coalition of the willing," as exemplified by various international partners supporting the United States invasion of Iraq. A coalition of the like-minded is based on similar values, produces policies based on those values, and presents more than a subtle shift in how the United States will approach its relationships with other states in this important area.

V. *An Unintended Legacy?*

Determining which lessons a country's leadership should learn from its experiences in dealing with a complex, violent, and adaptive adversary is difficult enough; determining the real lessons it has digested and begun to implement through the promulgation of policy and doctrine is even harder. This analysis is further complicated when the government's positions and guidance are pitched at the strategic level and are designed potentially both to educate friendly actors as to how it intends to plan, train for, and conduct its operations and to inform potentially unfriendly actors where redlines, or thresholds, might exist regarding their behavior towards that government and its interests, and its range of possible responses. Different government agencies will likely have different perspectives on the same event, and staffing processes within separate bureaucracies—ever mindful of parent agency priorities—might not lead to objective and consistent assessment of what is truly worth learning and applying. These two strategies may be decent candidates for staking out exceptions to this rule, however. Both appear to have been built in a holistic fashion, concerning an area internationally recognized as being of crucial importance, with the benefit of a decade's worth of successful and

[53] Letter from John Yoo, Deputy Assistant Attorney Gen., to Alberto R. Gonzales, Counsel to the President 6 (Aug. 1, 2002), *available at* http://news.findlaw.com/wp/docs/doj/bybee80102ltr.html.

unsuccessful experiences on similar and related issues. On this basis, the cyberspace strategies are not just policy pronouncements; they are likely complementary statements of underlying values and practical priorities reflected across the breadth of an Administration's engagement on the topic. If this is indeed a legacy of 9/11, even if an unintended diploma after an expensive and often painful tuition, the question remains whether the United States will be safer from terrorist attacks because it will conduct its foreign affairs and military operations in conformance with this approach. Holistic strategies particularly require holistic assessment, and holistic assessment is neither inexpensive nor simple. It requires a significant amount of time to register actual effects as compared to trends.[54] How successful the United States is at achieving its specific cyber goals, however, possibly could serve as a touchstone of the efficacy of this approach.

[54] *See* Rietjens et al., *supra* note 49, at 335–37 (addressing challenges in accurately conducting holistic analysis in complex environments).