Crossing the Line: Law of War and Cyber Engagement - The U.S. Position

Philip O'Neill Jr.

Follow this and additional works at: https://scholar.smu.edu/til

Recommended Citation
https://scholar.smu.edu/til/vol51/iss3/9

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in International Lawyer by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
Crossing the Line: Law of War and Cyber Engagement—The U.S. Position

PHILIP D. O’NEILL, JR.1

I. Introduction

The basic U.S. policy regarding the applicability of the law of war to cyber engagement is of recent vintage, articulated largely during this decade, impelled as the range of actions and actors on the threat continuum evolved with increasingly acute results.2

To begin to meet the challenge of cyber competition yielding to conflict, in 2011 President Obama recognized as a matter of declaratory policy in his “International Strategy for Cyberspace”3 that “[l]ong-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace.”4 That said, President Obama’s policy pronouncement also cautioned that: “unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them.”5

A legal and political policy debate over cyber “acts of war,” “use of force,” and “armed attacks” ensued in recent years, with the notion of “equivalence” to traditional military force triumphing doctrinally through adoption of an “effects-based” standard. Reduced to essentials, we gauge attacks, including those perpetrated through cyber operations, by their consequences, not the means of delivery. This evaluative approach was desirable both for what it prohibits and for what it permits as a two-edged sword. According to public acknowledgement by former Chairman Dempsey of the Joint Chiefs of Staff, the U.S. had not declared exactly what kinds of cyber-attacks and what

1. This article is based upon a presentation by Mr. O’Neill at the ABA Spring meeting of the International Section in Washington D.C. on April 26, 2017, available at https://static.ptbl.co/static/attachments/150017/1495047643.pdf?1495047643. Mr. O’Neill taught Nation Security Law at Boston University Law School, and is the author of books on national security law and arms control published by Oxford University Press. He presently serves as co-chair of the ABA International Section’s National Security Law Committee.
4. Id. at 9.
5. Id.
level of damage hits the threshold of an “act of war.” The position received an updated confirmation in June 2016 in testimony before the House Armed Services Committee; then acting Department of Defense (DOD) Assistant Secretary for Homeland Defense and Global Security Atkins confirmed that a cyber-strike as an act of war “has not been defined. We’re still working toward that definition.” His testimony was the same as to a lack of definition when asked about state or non-state actor cyber-attacks against civilian targets with “significant consequences.”

The Trump administration, pursuant to Congressional direction, submitted a classified national policy for cyberspace and cyber warfare in April 2018. Little has emerged since then publicly. In April 2018, testimony before the House Armed Services Committee, former DHS Secretary (and DOD General Counsel) Jeh Johnson observed in testimony at hearings on information warfare below the traditional level of armed conflict that: “Under what circumstances can a cyberattack constitute an act of war? At the moment there is no legal definition for the term. Essentially, the answer from [legal scholars] and me, is “maybe,” or “it depends” or “we will know it when we see it.” Most recently, in a reported remark that did not even warrant a headline, General Paul Nakasone, the head of the National Security Agency and U.S. Cyber Command, stated (apparently without qualification) at an Aspen conference that “cyber attack from

---


another government on U.S. critical infrastructure would cross the threshold into war, ‘and we would certainly respond.’”

In those circumstances, how do our officials measure malicious cyber incidents for appropriate response, particularly those of non-state fronts and cut-outs? When does the DOD take the governmental lead in responding to a cyber-attack? How and where does that lead us and others in discerning “when the line is crossed.” In other words, when does a cyber-war start and precisely how are we supposed to know it?

The short answer is not missing in action; rather, as a matter of official policy, hitherto we basically had criteria for evaluation, which are applied on a case by case, fact-specific basis for serious cyber incidents by the President and his national security team. As the former Deputy Assistant Secretary of Defense for Cyber Policy, Aaron Hughes, observed in the “Digital Acts of War” hearings in July 2016 before the Subcommittees on Information Technology and National Security of the House Committee on Oversight and Reform:

[When determining whether a cyber-incident constitutes an ‘armed attack’, the US Government considers a number of factors, including the nature and extent of injury or death to persons and the destruction of, or damage to property. As such cyber incidents are assessed on a case-by-case basis and, as the President has publicly stated, the U.S. Government’s response to any particular cyber incident would come in a place and time and manner that we choose.

It suffices to say that these criteria were offered in lieu of rather than as “red lines” delineating exact thresholds of behavior triggering “use of force.” In sum and substance, that was the testimony on July 13, 2016 of State Department official Christopher Painter, then the Coordinator of Cyber Issues, in those same hearings. He further explained that this is really no different than the historic position of the U.S. and other nations, which have refrained from “defin[ing] precisely (or stat[ing] conclusively) what situations would constitute armed attacks in other domains and there is no reason cyberspace should be different.”


PUBLISHED IN COOPERATION WITH SMU DEDMAN SCHOOL OF LAW
of proof to be required — a matter of some import, as history in this century informs us.

Thus, we have a traditional standard and we have applicable evaluative criteria. But as Acting DOD Deputy Assistant Hughes also acknowledged to the House Armed Services Committee in July, 2016 in other cyber warfare hearings: “We just don’t have guidance on application to scenarios.” That is a bit of an of an overstatement, but not by much. Drilling down somewhat into the public record to see what examples we and others, including potential adversaries, do have to base decisions on, there is minimal substance or clarity to be found. The initial illustrative examples flowed from former Legal Advisor Koh’s explanation in a scripted, inter-agency commentary in September 2012, that cyber activities that proximately result in death, injury or significant destruction “would likely” be viewed as the “use of force.” By analogy with kinetic weapon parallels, he specifically likened the effects of cyber operations to those of kinetic attacks upon a nuclear power plant, which melted down, or bombing a dam in a populated area, or disabling air traffic control so that a plane crashed. Similarly, the DOD observes in the most recent edition of its Law of War Manual, that where cyber operations against military logistics systems crippling impede the ability to conduct and sustain military operations, that “might equal a use of force.” At the same time, the Manual also provides examples of factors indicating when a cyber-operation does not amount to an “attack” under the Law of War (Section 16.5.2), such as when a cyber-operation only causes reversible or temporary effects.

Accordingly, per the Manual, actions amounting to minor or brief disruption of internet services, or the brief disruption, disability, or interference with communications do not qualify. In that regard, one might inquire how “temporary” is defined. For example, the U.S. experienced a significant Distributed Denial of Service (DDOS) attack on October 21, 2016 that brought down many prominent sites for much of a

17. Id.
19. Id. at 996.
20. Id.
day, with considerable economic consequence. In comparison, we also know that the Russia-sourced cyber-attack on Estonia in 2007 took down the internet there for two weeks, but Estonia did not seek to invoke Article 5 of the North Atlantic treaty for collective defense. Even a June 2017 attack, attributed by the White House Press Secretary to the Russian military and dubbed as the most destructive and costly cyber-attack in history, was not characterized as an “act of war” — economic or otherwise. Indeed, it was mentioned almost in the same breath of subsequent Congressional testimony as the observation that “we are in the midst of a ‘very real series of (minor) military squirmishes’ in cyberspace.” In comparison, no less of an authority than the President of the United States in late 2014 publicly branded the North Korean attack on SONY as an “act of cyber-vandalism,” and expressly disclaimed it as an “act of war”. Nevertheless, this direct attack on American civilians by a foreign power was publicly acknowledged in the DOD’s cyber strategy as “one of the most destructive cyber-attacks yet on a US entity”.

Further articulation of applicable criteria for the “effects-based” standard and application of the law of war has, to date, largely been delivered through a combination of executive orders and statements; Presidential Policy Directives; Departmental Strategy and Policy Statements and Reports; as well as public remarks by senior officials — often reactive in event-driven circumstances — and in their testimony before Congress. Additionally, further insight may be derived by logical implication from our command and control structuring for cyber operations. The process also is now being driven in part by Congress, pursuant to annual DOD funding authorizations, particularly in Fiscal Year 2017 and again for 2019. So, what can be gleaned from all of these sources?


II. The Development (and Export) of the US Legal Position

The DOD, in the 2010 Quadrennial Defense Review, identified cyberspace as a global commons and domain. This recognition followed purported Russian cyber activity in Estonia in 2007 and Georgia in 2008, as well as our own experience with it from Serbian cyber-attacks in 1998 and reported use by Israel in its attack on a Syrian nuclear reactor in 2007, among other cyber activity in a political/military context. Against this background, in May 2011 the DOD issued a “Strategy for Operating in Cyberspace” which expressly recognized cyberspace as an operational domain equal to those of land, sea, air and outer space. The DOD also specifically, albeit generally, acknowledged that computer sabotage by another country could constitute an “act of war.”

With respect to the development of US declaratory policy on the intersection of cyber activity and applicable law, the “effects-based” prism through which we now view any “use of force” or an “armed attack,” drew upon the conclusions of leading legal scholars in the area working on it since the 1990s. It also found official recognition at the DOD as early as May 1999, in the “Assessment of the International Legal Basis in Information Operations.” There, the DOD General Counsel observed that “the international community is more interested in the consequences [of an attack] than its mechanism,” in suggesting that cyber operations could constitute armed attacks giving rise to the right of self-defense. Hence, the results of attacks, rather than means, matter most in all physical and virtual operating domains.

29. See, e.g., Jason Healey, Cyber Attacks against NATO, then and now, ATLANTIC COUNCIL (Sept. 6, 2011), http://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now.
35. Id. at 18.
U.S. cyber law views are also shaped within the context of long-standing U.S. articulation of its construction of applicable U.N. Charter Articles (e.g., the inherent right of self-defense potentially applies against any illegal use of force). U.S. positions were largely developed in the context of the Cold War, when U.S. policymakers and diplomats emphasized the might of arms as a trigger, as opposed to different forms of coercion (economic; diplomatic or otherwise) championed primarily by less powerful and developing nations. Whether past restrictive views of “use of force” will continue in the cyber context will most likely be tested in the future by “disruptive” attacks. Even in the absence of physical destruction, they can have serious economic impacts, particularly if directed at critical infrastructure sectors. Such attacks can be relatively enduring and at such a scale — even if shy of a “significant consequences” threshold — that those unique aspects may eventually give us pause for consideration of the continuing viability of past interpretation of “use of force” in such circumstances.

Doctrinally, the current U.S. position was largely memorialized in the most recent revision of the DOD Law of War Manual, as noted above. The Manual also generally identifies and describes the international legal architecture applied to military cyber activity.36 There, one finds acknowledgement that the law of war rules are not framed in terms of specific technological means, and are not well settled on precisely how they apply to cyber operations.37 Perhaps that ambiguity will invite the kind of “supplementation” expressly contemplated in President Obama’s 2011 Cyber Strategy to address seriously disruptive cyber activity—whether in isolation—or more likely, cumulatively.38 After all, international and domestic lawyers alike are familiar with principled exceptions to many rules, and the cyber area may prove to be no different in that regard as well. Presently though, such disruptive activity does not “cross the line” under the US position, consistent with past Charter Article 2(4) interpretation.

In any event, by September 2012, Legal Advisor Koh (as previously referenced) articulated the consensus view on how we apply old laws of war to new cyber circumstances. First came confirmation that existing international law principles do apply in cyber-space; it is not a “law-free” zone.39 This recognition is really no different than that which occurred with other technological advances in the past, such as the airplane’s impact on warfare, or the opening of new physical domains, including outer space with restrictions and, in contrast, peaceful use of Antarctica. These were all areas or technological advances where the need to account for change arose in the last century. Additionally, the September 2012 commentary expressly recognized that cyber activities can constitute a “use of force” under U.N. Charter Article 2(4), with the national right of self-defense per Article 51 potentially triggered by cyber activities that amount to an “armed attack” or

36. See LAW OF WAR MANUAL, supra note 18.
37. See id. at 988-99.
imminent threat thereof.\textsuperscript{40} Further, U.S. recognition at that time acknowledged that the law of armed conflict applies to regulate use of cyber tools in hostilities.\textsuperscript{41} Related principles that apply include those of distinction; limitations through necessity and proportionality; limitations on indiscriminate weapons; as well as state sovereignty, including attribution through “control” of proxies. The current DOD Law of War Manual echoes these views, which retain continuing vitality in the cyber domain.\textsuperscript{42}

The State Department also took the lead in various international forums in recent years to promote a consensus among allies and other states on the applicability of international law generally to cyberspace, as well as in efforts to develop recognized norms of acceptable/unacceptable peacetime behavior in cyber space, together with confidence building measures (CBM). The State Department’s multilateral efforts to develop cyber principles seeks to reduce risk of escalatory spirals. These efforts were recognized in the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. For example, the U.N. Group in a 2013 report affirmed the applicability of international law and the U.N. Charter to cyberspace.\textsuperscript{43} In 2014-15 the UN Group affirmed the inherent right of self-defense under Article 51 in cyberspace.\textsuperscript{44} Another highpoint came in November 2015 with the issuance of the G-20 Leaders Communique in which G-20 Leaders affirmed that international law, and in particular the U.N. Charter, is applicable to state conduct in the use of information and communications technology.\textsuperscript{45} It is fair to say the cyber norm and CBM-building effort by the State Department emerged as a U.S. foreign policy imperative in such forums in the Obama years. A focal point in the prior international consensus building effort of the State Department was establishing voluntary peacetime norms in which key areas of cyber risk, such as critical infrastructure, are identified and placed “off limits” to hostile cyber operations. That effort found successful recognition in the 2015 Report of the U.N. Group of Experts,\textsuperscript{46} but not operationally in the digital world.

In comparison, the Trump administration has repeatedly de-emphasized cyber issues in foreign policy thus far. From the State Department’s closure

\begin{itemize}
  \item [40]\textit{Id.} at 3-4.
  \item [41]\textit{Id.} at 4-5.
  \item [44]\textit{Id.} at 12.
\end{itemize}
of a dedicated cyber-security coordination office, to current National Security Advisor John Bolton’s parallel elimination of the cybersecurity coordinator position on the National Security Council, the current administration has been consistent on this front. Whether these actions signal a complete diplomatic retreat, is open to interpretation. The two summary public reports, totaling eight pages, released by the Office of the Coordinator for Cyber Issues in late May 2018, provided no clear answer in this regard, and only the most general recommendations to the President on protecting cyber interests and the American people. But these and other actions are appropriately viewed as an indication of an impending policy shift toward exploiting ambiguity, rather than seeking to limit it. Indeed, the reported replacement of an Obama era Presidential Policy Directive with a new classified one that grants far more latitude for offensive use of cyber actions, appears to confirm the conclusion that exploitation is now the preferred path to achieving deterrence that proved so elusive under the prior restrictive reaction and norm building approach.

Still, a dual track approach of parallel legal efforts in military forums met with considerable success over time in embracing the U.S. position. For example, NATO cyber defense policy evolved to recognize the applicability of international law to cyber space. This was manifested both in the general declaratory policy of NATO as in the more detailed explication of cyber operations and the law of war produced by the group of experts convened by NATO in 2009, who delivered the Tallin Manual in 2013 on the application of international law to cyber operations, and the 2.0 version

---


48. There has been some effort legislatively to counter these re-organization efforts. See, e.g., Joseph Marks, Lawmakers Take Another Shot at Transforming Trump Cyber Policy, NEXTGOV, June 11, 2018, https://www.nextgov.com/cybersecurity/2018/06/lawmakers-take-another-shot-transforming-trump-cyber-policy/148999/.


earlier this year (which goes into much greater depth on evaluative criteria). From the standpoint of declaratory policy, NATO has acknowledged publicly, since September 2014, that (i) international law applies in cyber space; (ii) cyber defense is part of the core task of collective defense; and (iii) hostile activity in cyberspace can potentially trigger Article V obligations where the effects are comparable to those of a conventional attack. Such invocation determinations are made by the North Atlantic Council on a case-by-case basis. There is alliance recognition that “cyber-attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability.” Where that line is to be drawn awaits further elaboration or experience. In any event, NATO affirmed in July 2016 that cyberspace is a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. At that time, the NATO Secretary General also publicly declared that a “severe” cyber-attack may be classified as a case for the alliance and, further, that the members intend to respond to any assault, including a cyber-attack that could be classified as an “act of war.”

III. The U.S. Command Structure as a Reflection of Where the Line is Crossed

Along with general recognition of the need for and efforts to establish shared voluntary normative cyber behavior in peacetime, as well as adapting common understandings of it in the law of war, came recognition of the deficiencies in our organizational structure for response. Addressing this deficit results both in alerting others where we stand for deterrent purposes, as well as in establishing the operational architecture of how our own command and control would be triggered and flow in the event of “attack” — which is often used in the cyber context in a colloquial sense, rather than to connote actual physical violence.

The US has certainly made known for deterrence purposes in its Cyber Strategy since 2011 that:

[w]hen warranted, the US will respond to hostile acts in cyber space as we would to any other threat to our country. We reserve the right to use all necessary means — diplomatic, informational, military and economic — as appropriate consistent with applicable international law,

55. Id. at ¶72.
in order to defend our Nation, our allies, our partners, and our interests.58

There was also a caveat in the public fact statement59 — which achieved unintended full transparency when Edward Snowden made public in June 2013 Presidential Policy Directive (PPD) 2060 — that “[i]t is our policy that we shall undertake the least action necessary to mitigate threats and that we will prioritize network defense and law enforcement as preferred courses of action.”61 It appears that policy statement is now history. The directive itself was reportedly terminated (as this article went to press) and replaced by a new Presidential Policy Directive, the contents of which are as yet publically unknown.62

Still, this “whole of government” approach to response was embedded in the governance structure of dealing with cyber threats. In the six years following issuance of President Obama’s 2011 Cyber Strategy, the DOD, State and the Department of Homeland Security (DHS), acted in concert with other agencies, Congress, and increasingly with allies such as NATO, other like-minded nations, and even the private sector. The prior administration articulated general policies and endeavored to fill in some of the blanks to help establish the legal architecture for the cyber domain to provide some notice of the cyber trigger line, as well as a hierarchy of shared command and control of response. The results, which in some instances were reactive to circumstance, matured and moved well beyond an embryonic stage of development. Response procedures were in place,63 assuming that authority was recognized by agreement on the effects analysis. Since one of the criticisms of that structure was the unwieldy aspects of having “too many cooks” involved, presumably the new policy directive emphasizes a more streamlined approach, with attendant potential coordination issues64.

The issue remains, then, of how the latest refinement of the operational structuring of governmental and defense assets to address experience with malicious cyber activity below the act of war threshold will play out, including application of appropriate rules of engagement in response by the DOD and others. To that end, section 1632 of the National Defense Authorization Act of 2019 did seek to diminish inter-agency friction and
settle some issues with respect to Title 10/Title 50 debates regarding the Cyber Command’s conduct of operations outside of combat zones; it did so by affirming that clandestine military operations in cyber space “in areas where hostilities are not occurring” is traditional military activity within the Title 50 exception to covert action requirements.

The legislative clarification should help smooth operational activity, for our officials will likely continue to grapple with categorization and response to attacks of increasing frequency. This is so because “[w]e are vulnerable in this wired world” — to quote the DOD Cyber Strategy released in 2015. Ample alarm was previously sounded in detail about the extent of that vulnerability in the January 2013 Defense Science Board Cyber Report. Less than a month later President Obama issued Executive Order 13636 to strengthen U.S. policy to enlarge the security and resilience of the Nation’s critical infrastructure. That infrastructure was then defined generally as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” It is noteworthy that no express temporal component was publicly embedded as a qualification to an effect of “incapacity” in that definition, although one might be implied from the concept of “debilitating.” Still, the gauntlet was thrown down: what would be protected to give concrete expression within the definitional parameter?

To that end, on the same day in February 2013 as the executive order was released, Presidential Policy Directive 21 also was issued. Among other things, it provided greater clarity to the roles and shared responsibilities assigned to promote cyber defense, to be led by DHS, including the identification of sixteen critical infrastructure sectors. Implementation followed; assets were prioritized and vulnerabilities were and are being assessed. Cyber targeting of those sectors with “significant consequences” now carries a giant flashing caution sign to deter adversaries in peacetime;

---

69. Id. § 2.
70. Id.
72. See id.
equally though, it potentially helps them prioritize preparatory steps for target selection in time of war.74 Indeed, the continuing extent of that sector’s vulnerability was confirmed recently in Senate hearings early in 2017 by the Chairman of the Defense Science Board, who observed that our critical infrastructure vulnerability to major adversaries’ cyber offenses will exceed our ability to defend for at least the next decade75 — hence the public elevation in import of deterrence. It suffices to say that since 2013 the Director of National Intelligence (DNI) has named the cyber threat as the number one strategic threat to the US, ahead of terrorism76 — with good reason, as Ex-Joint Chief Chairman Dempsey publicly confirmed the multi-fold rise in cyber assaults against critical sectors.77

In terms of “crossing the line” for DOD purposes, scenarios to consider continue to range from penetration efforts in critical infrastructure to prepare future battle fronts, to existing attacks on DOD and Defense Industrial Base cyber networks, to those of “significant consequence” to the sixteen civilian critical infrastructure sectors (as identified in PPD 21 and pursuant to it) and electoral systems infrastructure78. This range of activity may trigger DOD defense, as opposed to DHS control or that of sector specific agencies. There is no assurance that President Trump’s new Policy Directive will add sufficient clarity to responsibility assignment, particularly if the DOD is granted new operational authorities.79 One may still look for some guidance on where the “line is crossed” in the DOD’s most recent Cyber Strategy, as in future ones. Currently, there is general reference in that context to “loss of life, significant damage to property, serious adverse


76. See generally LAW OF WAR MANUAL, supra note 18.

77. General Martin E. Dempsey, U.S. Army, Gen. Dempsey’s Remarks and Q&A on Cyber Security and the Brookings Institute (July 27, 2013), http://www.jcs.mil/Media/Speeches/Article/571864/gen-dempseys-remarks-and-qa-on-cyber-security-at-the-brookings-institute/; See also id. at 10 (“The gap between cyber defenses employed across critical infrastructure and offensive tools we know exist presents a significant vulnerability for our nation.”); See also id. at 12 (“...cyber may be our nation’s greatest vulnerability, ...”).


79. TASK FORCE ON CYBER DETERRENCE, supra note 65, at 5.
U.S. foreign policy consequences, or serious economic impact on the U.S.”

Yet, in Congressional testimony in the summer of 2016, a DOD official could not answer a hypothetical question on whether loss of life resulting from a cyber-attack on the electrical grid that cut off power to hospitals, would cross the line of “significant consequence” — although he did volunteer that DOD assistance would be provided if DHS needed help, which provides some insight into the DOD domestic operational mindset. Such matters simply highlight the difficulty of applying the standard and concomitant impact on response operational control. Frustration with general criteria will surely mount, for if hypotheticals can’t be answered, there is also the added challenge arising from the absence of visible custom and practice in the cyber domain. To explain, so much of cyber operation is covert, clandestine, or by proxy operatives and activists— basically the equivalent of cyber “little green men” through use of “cut out agents.” In such circumstances it can be hard to see (and foresee) the myriad threats and operations that will trigger serious and harmful results, although we are building up too much experience to draw upon. Hence, state practice in the cyber domain is likely to remain relatively veiled in comparison to others. This impedes the development of customary norms of acceptable and unacceptable behavior through visible state practice. As a result, experts, the public, and Congress alike justifiably fear that deterrence is not being well served by generalities. In short, we have moved past theory and are confronted by practice. This is particularly the case with respect to “disruptive” cyber-attacks, and even more so for “destructive” ones — a distinction recognized in the 2014 Defense Quadrennial Review — below the “significant consequence” threshold, wherever that may be. Moreover, “attribution” of cyber “control” for Article 2(4) purposes now, as in the past — ranging from the Wars of National Liberation in the Cold War to today’s “low intensity conflicts” — remains an issue of fact and law. U.S. national technical means increasingly provide the answer, but not necessarily in real time, nor to the public.

The terrain of “disruption” with or without destruction, thus expands the attack surface on the cyber battlefront. It has emerged as the “soft spot” of choice in exploiting both our vulnerabilities and emerging defensive regime. It is a potential magnet in this new era of threat to our industry, which acts

80. Id.
82. O’Neill, supra note 74.
84. Id.
85. Id. at 37; see also U.N. Charter art. 2,4.
as a force multiplier for any adversary who seeks to inflict economic death on us by a thousand cuts. The attack on the Sands in February 2014 by Iran, and more publicly visible attack on Sony later that year by North Korea, both exemplify such attacks. These were the first destructive cyber assaults on civilian targets in the United States, which were ultimately attributed to nation states. Neither, of course, rose to the level of a crippling assault on U.S. critical infrastructure, but they are a wave of the future. Indeed, in February 2015, testifying before the Senate Armed Services Committee, former DNI James Clapper acknowledged publicly that: “[w]e foresee an ongoing series of low-to-moderate level cyber-attacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security.” This represented something of a shift in focus from prior concerns articulated by former Defense Secretary Panetta over a “cyber Pearl Harbor” paralyzing the country. Still, multiple high profile attacks occurred before April 2015, when Executive Order 13964 created a new, targeted authority for the U.S. government to respond more effectively to many serious cyber threats that don’t “cross the line.” This executive order focused not only on cyber-enabled malicious activities that harmed or significantly compromised the provision of services by entities in our critical infrastructure, but also extended even to the significant disruption of a computer or network of computers. Accordingly, its applicability could reach attacks such as those on the Sands and Sony. Thus, this added economic weapon helps extend our layered cyber national defenses to attacks that do not necessarily trigger a DOD led response. Additionally, though, as we seek to gauge the existing effectiveness of deterrence now and in the future cyber-security environment, we should pause to observe and acknowledge that it has worked thus far — to the extent that no catastrophic cyber-attack has been experienced yet by the American people, although one could well be in preparation through ongoing probing of our critical infrastructure of power grids and dams, for example. At the same time, we do know that there is adversarial capacity to engage in cyber acts that no one would doubt constituted “acts of war” by their destructiveness from public acknowledgement by Ex-Joint Chiefs Chairman Dempsey.

86. Worldwide Cyber Threats: Hearing Before the Senate Select Committee on Intelligence, 114th Cong. 2 at 4 (2016) (statement of James R. Clapper, Director of National Intelligence).
87. Id.
88. Id. at 2.
91. Id. § 1(a)(C).
92. Cf. id. § 1(a)(A) with id. § 1(a)(C).
Still, there has been some general line drawing from an operational standpoint from which we and others can glean insight on what cyber actions may “cross the line”. The question of which types of attacks will likely be regarded as “acts of war” has been the subject of at least brief commentary by top officials in the past administration, who periodically endorsed U.S. general policy approach with some explanation. In particular, former Secretary of Defense Ash Carter, in his Drell Lecture at Stanford, was asked about the “low end of the threshold of significant consequence” that would trigger DOD involvement in the response hierarchy.94 His reply:

Something that threatens significant loss of life, destruction of property, lasting economic damage to the people. Any such use of force against America or American interests where the President would determine what the response ought to be on the basis of its proportionality and its effectiveness. It won’t be any different in cyber than it will be in any other domain — with the response not limited to the cyber domain.95

The answer does add a temporal component not expressly present in the sector definition of Executive Order 13636. Regardless, the temporal component of “lasting” might benefit from further elaboration to clarify when it is not “temporary” as the DOD Manual references.96 On the other hand, creative ambiguity both masks and maximizes executive discretion to deal with cyber confrontations, even if does not fix a precise declaratory line in the sand that cyber adversaries knowingly cross at their own risk.

We also have a qualitative guidepost to “line crossing” from public testimony three years ago by then Assistant Secretary of Defense for Homeland Security and Global Affairs Rosenback before the Senate Armed Services Committee. He acknowledged that the DOD is expected to take the lead authority only on the most serious cases — about the “top 2% of attacks,”97 with responsibility at DHS, Treasury or the sector specific lead agencies for the other 98%. We also know from that testimony that it would not include DOS cyber-attacks, “unless it would cross the threshold of armed attack in most instances.”98 Where is the line drawn? As then Secretary Carter somewhat obliquely referenced at Stanford, if a U.S. cyber-attack is one which the President must authorize (and for which pre-decisional operational plans are already in place), the United States certainly

96. See id.
98. Id.
has another internal guidepost from it on what would likely be regarded as an “armed attack” against the U.S. We do not know, nor do our adversaries yet, whether the new Presidential Policy Directive will change the DOD trigger point, or simply authorize a more flexible operational response when it is reached, or both. Certain adversaries do know, however, that Section 1642 the 2019 National Defense Authorization Act, signed by the President on August 13, 2018, grants Congressional pre-authorization for an active “proportional” DOD cyber response against them if authorized by the National Command Authority (the President and Secretary of Defense). That Congressional authorization requires as a rule of construction a “systematic, and ongoing campaign” of cyber attacks, including attempts to influence our democratic processes, by Russia, China, North Korea or Iran. This authorization, if utilized, would seemingly task the DOD at levels below the threshold acknowledged just a few years ago.

Further, we previously knew from PPD 20 that with respect to cyber operations directed at our critical infrastructure:

> [s]pecific Presidential approval is required for any cyber operations including cyber collection, DCEO, and OCEO - determined by the head of a department or agency to conduct the operation to be reasonably likely to result in “significant consequences” as defined in this directive. This requirement applies to cyber operations generally, except for those already approved by the President. . . .”

The definition of “significant consequences, under the former directive was “[l]oss of life, significant responsive actions against the United States, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States.” PPD 20 also previously authorized emergency cyber action by the Secretary of Defense, or authorized department agency heads pursuant to procedures authorized by the President, if such authorization was needed, to conduct emergency cyber actions necessary to mitigate an imminent threat or ongoing attack using defense cyber effects operations (DCEO) if circumstances did not permit obtaining prior approval. This delegation of authority also was measured under a standard of matters involving imminent loss of life or significant damage with “enduring” national impact to essential functions of government, critical infrastructure, key resources, or the mission of U.S. military forces. There were other conditioning factors, including among them, that the emergency action be necessary in

101. Id. § I.
102. Id. § V.
103. See id.
accordance with the inherent right of self-defense under international law and, further, that the DCEO not be likely to have “significant consequences” nor be lethally intended.\textsuperscript{104} The U.S. Government was also previously instructed to conduct DCEO with the least intrusive methods feasible to mitigate a threat.\textsuperscript{105} In PPD 20, the temporal component missing in the subsequent publicly released Executive Order 13636 was found, which provided the missing link of executive gloss on how to measure consequences.\textsuperscript{106} What the new Presidential Policy Directive does in this regard is classified, as was its predecessor until Snowden released it publicly.

In any event, our own contemplated cyber attacks with “significant consequences” had a top level command structure similar to that of nuclear weapons. Based on the delegation authority provided in PPD 20, one might surmise that a cyber-delegation of command or devolution of control structure is in place in the event of emergency or catastrophic attack (similar to that for nuclear attacks).\textsuperscript{107} Former Joint Chiefs Chairman Dempsey publicly confirmed the existence of pre-decisional emergency response procedures.\textsuperscript{108} At the same time, he also acknowledged the ongoing revision of cyber rules of engagement. Still, it is noteworthy that the then head of the US Cyber Command, Navy Admiral Mike Rogers, publicly expressed in February 2017 the hope that greater tactical delegation of cyber weapons will be afforded to commanders in the five to ten year range, as presently outside a defined area of hostilities is controlled at the executive level and not delegated down, except in certain circumstances.\textsuperscript{109} His view was that with greater experience, greater confidence is expected to be engendered to push offensive cyber capabilities down to the tactical level.\textsuperscript{110} Whether that operational timetable was actually advanced by the new Presidential Policy Directive is currently unknown outside the Executive branch and responsible Congressional oversight committees. But any necessary Congressional clarification as to the authorization process for such clandestine cyber operations, as noted above,\textsuperscript{111} is found in section 1632 of the 2019 National Defense Authorization Act’s confirmation that it is Title 10 traditional military activity, so it may well be felt by virtual adversaries already. In any event, DOD cyber operations will more closely resemble special forces activity for oversight purposes. After all, the legislation that created our cyber military force several years ago, and which very recently

\textsuperscript{104} See id.
\textsuperscript{105} Id. § III.
\textsuperscript{107} Id.
\textsuperscript{108} General Martin E. Dempsey, U.S. Army, A Discussion on Cybersecurity with General Martin E. Dempsey at 36-37 (June 27, 2013).
\textsuperscript{110} See id.
\textsuperscript{111} See TASK FORCE ON CYBER DETERRENCE, supra note 65, at 5.
empowered and elevated it to a unified command, with a direct report to the Secretary of Defense (rather than commander of our strategic forces), was closely modeled after the much earlier 1980s legislation with respect to our Special Operations Command.

Importantly, from the standpoint of fixing the demarcation line for cyber-attack, the 2017 Defense Authorization Act also sought to improve cyber deterrence by pushing the fiscal button on how the United States responds. Rather remarkably, it sought to do so by impelling the Secretary of Defense and Chairman of the Joint Chiefs of Staff to provide a list of military and non-military options available to deter or respond to malicious cyber activities, and a list of rules of engagement and operational plans to execute options. Given the then existing regulatory limitation on DOD response to cyber events outside its own and DIB systems, the logical focus of such plans would be tied to significant consequences to our critical infrastructure, and not to 98% of the disruptive and less destructive attacks on U.S. networks — unless that threshold for DOD involvement changed, with the engagement “line” drawn at a lower threshold, or through shared responsibility granted to DOD to provide assistance. Armed with that list, the President was then required by law to articulate when and in what circumstances he would authorize the execution of the options.

As such, the FY 2017 Defense Authorization Act was the successor to the legislation introduced in 2016 by Senator Rounds pursuant to which “digital acts of war” were to be defined to better, deter, and enable the DOD to respond. That proposed legislation was resisted by the Executive Branch and not well received by Congress. While the then DIA Director in Senate testimony on February 9th, 2016 observed it would be helpful to have a clear definition of both a cyber act and an “act of war,” it is one thing to task our DOD acting in concert with other governmental entities with analysis of which attacks are catastrophic or destructive enough to define it as an “armed attack,” it is quite another to give a specific “heads up” to adversaries about it for deterrence purposes. Certainly, highly classified and unclassified versions of the report were anticipated, but how deterrence is served is unexplained when where the line is crossed is undisclosed.

Still, we do see “notice” or “signaling” play out from time to time and in various alternative ways in the cyber warfare sector. That is well illustrated by the public observation on June 10, 2016 when a ranking member of the House Permanent Select Committee on Intelligence stated that an attack on a U.S. satellite, such as strategic indication and warning systems, could be

115. Global Threats (C-SPAN television broadcast Feb. 9, 2016)(director of National Intelligence James Clapper testified before the Senate Armed Services Committee).
considered an “act of war”. But what significance, if any, does an adversary attach to such pronouncements if not echoed by the Secretary of Defense or President? There are similar parallels with recent pronouncements about Russian cyber forces by members of the Russia legislative oversight committees that invite inquiry into what significance to attach to them.

Nevertheless, after the previously referenced hearings and rejection of the “Cyber Act of War Act,” Congress sought to highlight the lack of specific policy and strategy for deterring, defending, and responding to cyber-attacks. With the FY 2107 Defense Authorization Act, Congressional intrusion into Executive branch prerogative through use of the purse strings surfaced seeking predetermined cyber security related decision making. Yet, it did not even draw ire from outgoing President Obama in his signing statement in December, 2016, but it seemingly will when push eventually comes to shove — constitutionally or otherwise — in the Trump administration. From a deterrence perspective, which purportedly impelled the legislative direction, one certainly cannot imagine that we will want such lists and options to see the light of day, so let us hope our cyber adversaries cannot hack into those lists and future reports. But given the inherent secrecy that need be accorded to such operational details, it is rather hard to see how deterrence is served, because historically it is accomplished by visibility to adversaries; that is, either by declaratory policy in which clear lines are drawn, or by making transparent operational steps with weapons or force deployment as a tangible and visible sign of transgression. In the cyber world where such visibility typically tends to be the least desirable option, it is a real challenge to deter acts that fall short of activity that all would tend to recognize as “crossing the line” such that they constitute a “use of force” or “armed attack” or “act of war.” In this regard, the “visibility deficit” was not filled by President Trump’s classified report to Congress in April 2018 on national policy for cyberspace and cyberwarfare. That report filed pursuant to the requirements of the FY 2018 National Defense Authorization Act may communicate Executive Branch intentions to our legislature on military led cyber operations, but it will only communicate to adversaries by implementation of those policies. Ultimately, it would seem that “signaling” where precise lines are drawn will be in cyberspace through action; not through public discourse, other than continuing

Congressional monitoring120 and expressions of disappointment with past responses of the executive branch to adversary cyber attacks121.

IV. The Import of Recent Cyber Operations to “Crossing the Line”

We may have hit upon something of a solution to the deterrence dilemma, in demonstrating our cyber capabilities to a certain extent that could be leveraged now and in the future as a credible threat for deterrence purposes. In the recent past we actively and admittedly engaged in offensive cyber warfare operations against ISIS. It is, after all, easier to attack an entity that is not recognized as a sovereign, than it is to attack a full blown nation state. The point remains that what we were doing was engaging in cyber warfare — “dropping cyber bombs” to quote our Ex-Deputy Secretary of Defense Bob Work.122 Our cyber-attack was conducted in the context of our fight with ISIS, and was said by our former President and then top DOD officials to be directed at its “command and control network.”123

That concept usually triggers a direct military association with respect to impairing oversight and direction of forces and weapons. With respect to ISIS, we know from former Secretary of Defense Carter’s remarks at a press conference that our cyber capabilities being exercised go beyond jamming in traditional electronic warfare. They extend to operations calculated to promote loss of confidence by the enemy in their network, overloading it and reportedly doing “all of these things that will interrupt their ability to command and control forces there, control the population and the economy.”124 Now the novel magic in that formulation relates to the “population control and the economy” addendum (which was not reported in all news accounts) — matters that we historically have tended to think of as “governance” rather than “command and control”. If it is the case and the U.S. took a more expansive view of “command and control” by encompassing those governance sectors, then depending upon what we did and how visible it was to adversaries like Russia, there was increased insight into what constitute cyber “use of force” and an “armed attack.” Where the effects can be monitored by the intelligence services of existing or potential...
adversarial regimes, that serves to remove doubts about our force structure, capacities, and political will to engage them. Perhaps, though, any conclusions are best not entirely separated from context — as with the Russian based cyber-attack on Ukraine’s power grid — which directly impacted the civilian population, but which came in retaliation, one must add, for good old-fashioned sabotage by physically bombing the power lines going into Crimea the month before. In assessing when the “line is crossed” by cyber operations, context clearly does matter.

In any event, despite all of the efforts to promote standards, identify criteria, and apply traditional international law to considerations of what constitute the “use of force”, “armed attack”, or “act of war,” we still differ when lines are drawn with such precision that matters perhaps falling short of the stated criteria are nonetheless very serious actions by sovereign and other adversaries. Most recently, with respect to the Russian cyber intrusion into our electoral process, top leaders in our defense establishment differed over whether such action against something as fundamental to Americans as the integrity of our electoral process constituted an” act of war” — which was Senator McCain’s reported view, or an “aggressive act” — which was Secretary Carter’s response when apprised of the remarks of the Chairman of our Senate Armed Services Committee. Clearly a line was crossed in the context of intelligence operations through the release and subsequent misinformation campaign. Whether a line was crossed in terms of a “use of force” determination or “act of war” is quite another matter. Still, for as much progress as we have made in this decade about when the “line is crossed,” our work is not done yet; the DOD seemingly remains unsure precisely when it is tasked with response — even though it expressly recognized in the April 2015 DOD Cyber Strategy that “[t]he increased use of cyber-attacks as a political instrument reflects a dangerous trend in international relations.” On the other hand, President Obama publicly recognized on December 29, 2016 that increasing use of cyber means to undermine democratic processes here and abroad, warranted an economic weapon explicitly targeting attempts to interfere with elections. Accordingly, the President approved, amending Executive Order 13964 to authorize sanctions on those who: “tamper with, alter, or cause a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.”

---


128. See THE DOD CYBER STRATEGY, supra note 66.

authority, that President visibly sanctioned nine Russian entities and individuals.\[^{130}\] One concludes per the DOD Law of War Manual (section 16.3.3.3) if the Russian action was not the “use of force,” one may still take necessary and appropriate actions in response that do not constitute a use of force. The former President’s public actions were consistent with the restrictive response policy previously articulated; whether there will be an “invisible” additional response is open to conjecture given the new Presidential Policy Directive.

In closing, the employment of such cyber attacks represents a continuing adversarial threat to our political order and democracy. The temptation is certainly there, on a matter of such fundamental importance, to fix sooner rather than later, where in the spectrum such matters fall on the line of hostile action to provide notice to adversaries — and to do so by design, rather than either by inadvertence or by reactive ad hoc additions to the response tool box for possible calibrated use. But given U.S. past history of intrusion in foreign governance and interest in “freedom to operate” in like fashion where national interest dictates around the globe, the issue bears wider policy consideration than just within the narrow confines of a debate over hostile acts of cyber intrusion. In the meantime, the rules of cyber warfare remain in development from a U.S. standpoint. But the United States continues to respond to cyber attacks against national interests when, where, and how it choses; using what it considers to be appropriate instruments of power; and acting in accordance with our view of applicable law and Presidential policy directive. While we have a cyber force structure as well as this administration’s “warfare” strategy and operational policy now in place, how it will all be actually employed in the “common defense” of our people when lines are crossed still remains a “work in progress.”\[^{131}\]

\[^{130}\] Id. § 2 (listing Russian entities and individuals).

\[^{131}\] See, e.g., the remarks of DNI Dan Coates in response to a question from Senator Mike Rounds in testimony before the Senate Armed Services Committee, 31 nt. 4-10 (Mar. 6, 2018), https://www.armed-services.senate.gov/imo/media/doc/18-20_03-06-18.pdf.