DOD LAW OF WAR MANUAL

Cyber Operations and the New Defense Department Law of War Manual: Initial Impressions

By Charlie Dunlap

With headlines in the aftermath of the OPM hack asking if it was a "cyber 9/11" or an "act of war," and *Lawfare's* own Jack Goldsmith's questioning the apparent "weak and hesitant" U.S. response to the hack, it may be helpful to take a look at a key legal resource: The U.S. Department of Defense (DoD) Law of War Manual, which, coincidently, was issued just last Friday.

What follows are some initial impressions about the Manual's cyber chapter (chapter XVI).

Background

First, a little context. The 1,220 page Manual is the end result of a nearly quarter-century effort, and one marked by almost interminable interagency squabbles. Indeed, the Manual – which is billed as the institutional view of only DoD – carefully caveats itself

RELATED ARTICLES

The OPM Data Breach: Congress Should Investigate, but Should Consider Its Own Responsibility for Protecting Federal Workers
John Bellinger Sat, Jun 13, 2015, 5:14 PM

Why The Weak And Hesitant Response to the OPM Breach?
Jack Goldsmith Sat, Jun 13, 2015, 10:48 AM

Proposed U.S. Export Controls: Implications for Zero-Day Vulnerabilities and Exploits
Mailyn Fidler Wed, Jun 10, 2015, 9:00 AM

Five Important (Or At Least Interesting) Provisions in the Intelligence Authorization Bill HPSCI Passed
Robert Chesney Mon, Jun 8, 2015, 11:00 AM

by saying that while other departments of the US government were consulted, it does not necessarily represent the position of the U.S. government as a whole. Still, there can be little doubt that it will constitute a very significant state-centered document that will serve as a much-needed counterpoint to nongovernmental organizations, academics, and others who have in recent years come to dominate the dialogue about the law of war.

Chapter XVI is entitled "Cyber Operations" - *operations* being a studiously less belligerent (and more expansive) appellation than *warfare* used for earlier domain-focused Manual chapters on "Naval Warfare" (chapter XIII) or "Air and Space Warfare" (chapter XIV). Though some may complain about its relative brevity (15 pages), the cyber chapter nevertheless represents another step in DoD's growing transparency about cyber operations generally. It was not long ago that most aspects of cyber operations beyond defensive measures were classified; in fact, DoD declassified the latest version of its rather benign Joint Publication 3-12 on Cyberspace Operations only last year.

That said, the Manual's cyber chapter itself relies considerably on the long-available 1999 DoD General Counsel assessment of the international law applicable to what was then called "information operations." Additionally, it draws heavily from former State Department legal advisor Harold Koh's 2012 cyberlaw speech. Given those pedigrees, many observers of DoD's legal approach to

The OPM Data Breach: Raising All Sorts of Government Enforcement and Privacy Protection Questions

Carrie Cordero, Paul Rosenzweig Sun, Jun 7, 2015, 1:30 PM

cyberspace operations may find that the chapter does not particularly break new ground, even as it reinforces and memorializes some(what) contentious differences with others in the international law community.

DoD's Manual makes it clear that it considers the existing law of war as generally applicable to cyber operations, but concedes that in the cyber realm the law is "not well-settled" and that aspects "are likely to continue to develop." This, together with an earlier statement in the Manual that its existence doesn't "preclude the Department from subsequently changing its interpretation of the law," gives DoD attorneys plenty of flexibility to further develop legal interpretations in the cyber arena.

For now, however, DoD largely sticks to accepted international law. For example, the Manual's position on peacetime cyber espionage is that to the extent "cyber operations resemble traditional intelligence and counter-intelligence activities, such as unauthorized intrusions into computer networks solely to acquire information, then such cyber operations would likely be treated similarly under international law" which is to say, not normally violative of international law (although almost always illegal under the domestic law of the target State).

Still, in a few instances the Manual deviates from widely-accepted interpretations of international law, to include some found in the influential Tallinn Manual on the International Law Applicable to Cyberwarfare. Although not necessarily reflecting the official NATO position, the 2013 document was sponsored by NATO's Cooperative Cyber Defence Centre of Excellence and is considered quite authoritative by most international cyberlaw experts. Nevertheless, there is not even a reference to it (but that may be simply a result of the fact that the cyber chapter – unlike other parts of the Manual - relies exclusively upon U.S. government sources).

Cyberattacks, the Use of "Force," and "Armed Attack"

Accordingly, one of the most interesting aspects to the Manual's cyber chapter is the position it takes as to what constitutes what is popularly called an "act of war" in the cyber domain. Of course, the text proper of the Manual never uses that political phraseology as it doesn't resonate in contemporary international law, but the underlying discussion of the necessary threshold of force "act of war" terminology generates is still critically important because it can determine whether the law of war applies, or whether a particular cyber event falls under a law enforcement legal regime.

At the outset, the Manual's cyber chapter clearly acknowledges that the many colloquial usages of "attack" in reference to some kind of cyber incident "are not necessarily 'armed attacks' for the purposes of triggering a State's inherent right of self-defense under *jus ad bellum*," and, for that matter, are "not necessarily 'attacks' for the purposes of applying rules on conducting attacks during the conduct of hostilities."

With respect to self-defense, the chapter re-asserts a view Mr. Koh enunciated in his 2012 speech, that is, that the U.S. considers "that the inherent right of self-defense potentially applies against *any* illegal use of force." (Emphasis added.) In other words, it rejects the proposition reflected in the 1986 International Court of Justice case of *Nicaragua v. U.S*. (and echoed in the Tallinn Manual) that there is a difference between "use of force" as used in Article 2(4) of the UN Charter and "armed attack" within the meaning of Article 51, the self-defense provision of the Charter, reserving the latter not for any and all forms of force as sufficient to use force in self-defense, but only the "most grave."

More specifically, the Tallinn Manual argument, which follows the *Nicaragua* logic, is that Article 51 requires a more egregious degree of force – typically involving death, injury or physical damage - before a kinetic defensive response is permitted. As Michael

Schmitt, the Director of the Tallinn Manual project admits, this difference in interpretation is where that manual departs from Mr. Koh's position and, now, the DoD Manual.

In expanding upon this discussion of what is essentially a restatement of the Koh speech, the DoD Manual introduces a bit of confusion. It declares that it is "likely" that if a cyber operation produces "effects that, if caused by traditional physical means, [it] would be regarded as a use of force." It goes on to provide examples that include a meltdown of a nuclear plant, opening a dam so as to cause physical destruction, or disabling an air traffic control system so as to cause a plane crash. The physicality of those illustrations would easily fit within the concept of "armed attack" as traditionally understood, and does not especially illustrate what kinds of lesser cyber incidents DoD would consider as sufficient to sanction a self-defense response.

In a footnote, the DoD Manual does quote from the Koh speech to further amplify how the U.S. would decide if a particular cyber event constituted a use of force. Koh said the U.S. "must evaluate factors including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues" in making such a determination. Again, not especially enlightening.

So what about cyber operations that do not, *per se*, directly cause the kind of death/injury/destruction in Koh's examples? The Tallinn Manual finds that there are activities amounting to "force" that do not involve such violence. Relying upon reasoning from the *Nicaragua* case, it indicates that a use of force within the meaning of the UN Charter could be as physically nonviolent as simply "providing an organized group with malware and training to use it to carry out cyber attacks against another State."

However, force so described would *not* – according to Tallinn - constitute an armed attack, and thus would not support using force in self-defense. Put another way, the Tallinn manual view (and the view of many international lawyers) is that a use of force that doesn't directly cause physical death/injury/destruction (or, as discussed below, loss of functionality) may violate Article 2(4) of the UN charter, but it is not ordinarily sufficiently analogous to an "armed attack" so as to activate the self-defense provisions of Article 51.

Given that the DoD's much more expansive view is that *any* use of force triggers a State's "right to take necessary and proportionate action in self-defense," it is unclear as to precisely what kind of cyber activity beyond those which directly manifest themselves in death/injury/destruction might fit DoD's conception of a self-defense authorizing use of force. One example in the cyber chapter may provide a hint. It states that "cyber operations that cripple a

military's logistics systems, and thus its ability to conduct and sustain military operations, might also be considered a use of force under *jus ad bellum*."

With that example DoD may be indicating an acceptance of a norm that cyber operations can cause coercive effects as grievous as any kinetically-defined "armed attack," even in the absence of the sort of physical consequences bombs and bullets normally produce. In this sense the Tallinn manual seems to be in accord as it appears to consider a significant loss of functionality (as in the DoD Manual's crippled military logistics system example) as possibly constituting an adequate degree of 'destruction,' so to speak, as to amount to an armed attack that could permit an Article 51 defensive-force response.

The DoD position as illustrated by the example is still significant because it shows that the U.S. defense establishment is plainly of the opinion that actual violence in no longer (if it ever was) necessarily required to constitute a legally-sufficient rationale for self-defense, cyber or otherwise. Professor Schmitt, who has long predicted such an evolution, recently pointed out that today even in the absence of death or destruction "shutting down the national economy is probably an act of war [armed attack]." He stipulates, however, that short of something of that scale, "we're not certain." It appears that DoD would likely agree.

Apart from everything else, the combination of the DoD Manual's "no threshold" for the level of unlawful force needed to trigger self-defense, along with the further view that the definition of "force" itself is not necessarily limited to situations where death or destruction result, may provide the kind of constructive ambiguity useful in deterring States if not other actors from cyber aggression. Adversaries cannot assume that a particular cyber activity will not bring down the collective wrath of the U.S. defense establishment, even if it would not be considered an "armed attack" by most governments.

For responses to cyber situations not amounting to a use of force, chapter XVI mentions countermeasures only in a footnote. Briefly, countermeasures are otherwise illegal actions pursued by a victim State in response to an illegal act (not amounting to a use of force) perpetrated by a hostile State. Countermeasures are rendered lawful in order to provide a victim State with a coercive means of halting illicit cyber activity by a perpetrating State. One countermeasure often discussed in the press is the "active defense" technique of "hacking back." Though cyber countermeasures, which cannot themselves amount to a use of force, have of late garnered some thoughtful discussion, they could nevertheless be problematic in the cyber context.

Like countermeasures, the concept of retorsion, which is an unfriendly but legal act in response to a malicious or hostile act not amounting to a use of force, merits just a single line in the Manual's text proper, even though the U.S. has already employed a form of retorsion – sanctions – in response to cyber incidents. However, the brevity with which countermeasures and retorsion are discussed is understandable not just because their appropriate application to cyber incidents is still developing, but also because the Manual is, after all, a law of *war* document, and these are legal devices principally pertaining to periods of putative peace.

Cyberattacks and Neutrality

Chapter XVI also embraces the application of the 1907 Hague Convention's rules on neutrality to 21st century cyber infrastructure. The Manual asserts that neutrals have no obligation to refrain from "merely relaying [a belligerent's] information" through their cyber infrastructure "provided the facilities are made available impartially." Furthermore, DoD takes the position that such routing through a neutral is not prohibited even if the data can be "characterized as a cyber weapon or otherwise could cause destructive effects in a belligerent State" so long as there are "no destructive effects within the neutral state or States."

The Manual's permissive approach to the application of traditional neutrality law to a neutral's cyber infrastructure might be indicative of how DoD views the issue of attribution in cyber incidents. Essentially, DoD seems to be warning other actors that just because a cyber attack may *emanate* from a particular country (e.g., lawfully relayed through a neutral's cyber infrastructure) that alone is not sufficient evidence to conclude that the attack *originated* there. Complicating the norm of attribution in this way not only reinforces an important aspect of the law of war, it also - as a practical matter - favors nations with sophisticated cyber-attribution capabilities.

Consequently, all of this could make particular sense in deterring potential cyber adversaries if DoD believes it has superior capacity to ascertain attribution in the cyber domain. In peacetime and wartime, cyber operations routed through third countries could present a legal and practical conundrum for the targeted State if it has less advanced means of determining attribution. At best, its ability to respond would be delayed. Conversely, the U.S. could, in essence, get inside an opponent's decision cycle if it has better forensic cyber skills. The resulting "decision superiority" is a marked military advantage.

So does the U.S. enjoy such an advantage? In a 2012 cybersecurity speech then Secretary of Defense Leon Panetta asserted that DoD had "made significant investments in forensics to address this

problem of attribution" and that it was "seeing the returns on that investment." Panetta then warned that "[p]otential aggressors should be aware that the United States *has the capacity to locate them* and to hold them accountable for their actions that may try to harm America." (Emphasis added). Notably, however, the Panetta speech is cited nowhere in the Manual.

How Cyberattacks are Carried Out

The Manual's view on the law applicable to the actual conduct of cyber attacks tracks closely with traditional law of war rules. For example, the DoD Manual states that "remote harms and lesser forms of harm, such as mere inconveniences or temporary losses, need not be considered in applying the proportionality rule." (The Manual elsewhere states the proportionality rule as precluding attacks where "the expected loss of life or injury to civilians, and damage to civilian objects incidental to the attack, would be excessive in relation to the concrete and direct military advantage expected to be gained," essentially mirroring similar language found in Article 57 of Protocol 1 to the Geneva Conventions to which the U.S. is not a party).

There are, however, some interesting nuances. As an example of the kind of "mere" inconvenience or temporary loss that need not be included the proportionality analysis, the DoD Manual describes a "minor, brief disruption of internet services to civilians." It

remains to be seen, however, what level of *ongoing* cyber inconvenience (e.g., a slower connection speed?) DoD might consider as being of the sort of annoyance so intrinsic to modern conflict as to *never* need to be considered in a proportionality analysis.

Furthermore, the Manual also asserts (somewhat incongruously vis-à-vis the previous discussion of "minor" and "brief" disruptions) that "economic harms" such as "civilian businesses in the belligerent State being unable to conduct e-commerce, generally need not be considered in the proportionality analysis." Since there is no "minor" or "brief" qualifications associated with that wording, it isn't clear if these economic harms are excluded even if they are significant and ongoing.

The answer actually may be "yes" given that chapter V of the Manual (entitled the "Conduct of Hostilities") expresses the view that "war-supporting," and "war-sustaining" entities are included in the U.S.'s interpretation of military objective, which are obviously not protected by the proportionality rule. In any event, the Manual nevertheless tempers these tough-minded and potentially controversial conclusions a bit by counselling that cyber operations "should not be conducted in a way that unnecessarily causes inconveniences to civilians or neutral persons."

Moreover, the Manual (again in chapter V) cites ratification statements of several allies with respect to Protocol 1 in adopting the view that the "military advantage anticipated from an attack" indicated in the proportionality rule "is intended to refer to an attack considered as a whole, rather than only from isolated or particular parts of an attack." This might justify, for example, a rather widespread and extended internet outage and malware attack simply designed to mislead an adversary into thinking that an offensive is strictly cyber in nature so as to magnify the surprise of major kinetic strike.

There are few direct references to cyber outside of chapter XVI. One of note is the mention in the context of lawful weaponry that there "would be few, if any, instances in which the use of a particular weapon system, such as precision-guided munitions or cyber tools would be the only legally permissible weapon." This is something of a counter to recent suggestions that there could be a cyber "duty to hack" as required means of limiting harm in armed conflict (the cyber chapter itself recognizes that using cyber capabilities may be "preferable as a matter of policy").

As the Manual indicates, some cyber capabilities are "fragile" and must be husbanded by commanders carefully as even a single use might allow an adversary to develop defenses that would render the

cyber technique "ineffective in the future." Accordingly, the notion of a "duty to hack" above what might be inferred from the existing law of war requirements finds little support from DoD.

Of course, the cyber operations' chapter shouldn't be read in isolation from other parts of the Manual. Thus, for example, chapter V discusses deceptions not technically prohibited by the law of war. Included as an example of a not-proscribed deception is the "false use of journalist credentials to feign civilian status" as a means of "feigning civilian status to facilitate spying or sabotage," something that may raise eyebrows if not consternation among the Fourth Estate. Although the Manual does not suggest the U.S. intends to do so, one could readily imagine any number of ways that cyber could facilitate feigning journalist status. This could further complicate the job of war correspondents and other reporters who already find themselves suspected of spying.

***

As indicated earlier, this brief analysis suggests that although the cyber chapter of the DoD Manual contains no earth-shattering legal propositions, it does a good job at gathering, organizing, and articulating views already on-the-record in DoD and elsewhere in the U.S. government, and this will no doubt be helpful to practitioners and scholars alike. To be sure, further analysis of the Manual will yield additional insights not just about cyber

operations, but also DoD's overall interpretation of the law of war. Make no mistake about it, law of war manuals make a vital contribution to warfighting, and this one is the most significant to appear in decades, if not ever.

Topics: Cybersecurity

Tags: cyber, DOD Law of War Manual, Law of Armed Conflict