CHAPTER 3


Sean Watts

1. Introduction

Almost simultaneously with its emergence as a domain of military operations, cyberspace presented substantial questions concerning the application and operation of international law. A considerable body of scholarship and doctrine now exists that addresses not only the relationship between cyberspace and international law but also likely and preferable paths of cyber law development. These sources include a wide range of positions and predictions on application and development that represent the full spectrum of international law outlooks and schools of thought.

In early treatments of the subject, a viewpoint emerged that might be termed Exceptionalist. According to this view, cyberspace represented an unprecedented novelty entirely unlike other domains previously regulated by international law. Exceptionalists imagined an Internet owned and regulated by no one, over which states could not and should not exert sovereignty. Some Exceptionalist views ran so strong that they issued manifesto-like declarations of independence that defied states to intervene.1 They advanced a view that Professor Kristen Eichensehr aptly termed 'cyber as sovereign'.2

The Exceptionalist view rested in significant part on a conception that emphasised the virtual characteristics of cyberspace. It comprehended cyberspace as a realm entirely apart from the terrestrial and therefore territorial world governed by international law. Exceptionalists noted that cyberspace is largely ambivalent to geography and political borders. They maintained that because interactions in cyberspace are virtual, bonds of nationality and aspects of territoriality were inadequate to justify the exercise of sovereignty by states.

In response to Exceptionalists, a view developed that might be termed Sovereigntist. According to the Sovereigntist view, cyberspace, while novel with respect to the conditions that informed the creation of most existing treaties and customs, remains fully subject to international law. The Sovereigntist view continues to recognise sovereign states as both the stewards and subjects of international law in cyberspace. Scholars sometimes refer in this respect to a ‘cybered Westphalian age’.

The Sovereigntist view rests on enduringly physical conceptions of cyberspace and an appreciation of the tangible components and groups or individuals that comprise its architecture. Cyberspace, Sovereigntists emphasise, is neither virtual nor metaphysical. It is simply a collection of processors and terminals, servers and nodes, cables and transmitters – all of which are located within territorial boundaries or zones controlled by sovereign states or regulated by international legal regimes. Sovereigntists highlight that cyberspace is also designed, created, programmed and operated by people – nationals of sovereign states who are fully subject to the jurisdictional regimes of international law.

These debates concerning the role of international law in managing cyberspace spawned a cottage industry of legal commentary and scholarship seeking to influence and shape future cyber law. Overwhelmingly resolved in favour of Sovereigntists, these debates were in large part conducted by and between non-state actors such as academics, non-governmental organisations, and think tanks. They produced commentary and claims that in both quantitative and qualitative terms have dwarfed the input of sovereign states.

As an example of highly influential work by non-state groups and in terms of comprehensiveness, the Tallinn Manual on International Law Applicable to Cyber Warfare (hereinafter Tallinn Manual) currently stands out from all other sources.

---

In 2009, the NATO Cooperative Cyber Defence Centre of Excellence invited an international group of law of war experts to address the state of international law applicable to cyber warfare. In a three-year project that included unofficial consultation with select states and non-governmental organisations, the group produced the Tallinn Manual which identifies, in the form of rules accompanied by commentary, a broad range of cyber norms and their accompanying international legal bases. With respect to the Exceptionalist/Sovereigntist debate, the Tallinn Manual falls squarely in the Sovereigntist camp. Indeed, its central thesis is that cyberspace does not negate the operation of the laws of war, either ius ad bellum or ius in bello.  

The Tallinn Manual limits itself with considerable discipline to descriptive assessments of the law and assiduously avoids prescriptive arguments or advocacy. Yet its comprehensive approach and inclusive format provide fertile ground for the seeds of prescriptive claims concerning emerging law and the development of future norms. Issues on which the group could not achieve consensus are treated by commentary that records majority and minority views on a wide range of controversial subjects for which cyber norms may be emerging. Although not its purpose, the Tallinn Manual has inspired calls for the development of new norms, especially those identified as unsettled or ambiguous in their current state.

Given their pervasiveness and in some cases persuasiveness, it is tempting to resort to the work of non-state actors, such as the Tallinn Manual authors, for indications of the future direction of the relationship between cyberspace and international law. Their work can easily be adopted or even mistaken as a proxy for the legal input of states. Yet the fact remains that states and states alone are responsible for and competent in the formation of international law. It will be their practices, their prerogatives, their perceptions, and, most importantly, their consent that will form future international cyber law.

In that vein, this chapter examines the recently released United States Department of Defense (DoD) Law of War Manual (hereinafter the Manual) as a sample sovereign view on the current state of international norms applicable to cyberspace operations and to assess state interest in the development of new cyber-specific norms. Although its focus is on cyber operations that rise to the legal thresholds associated with or conducted in the context of armed conflict, the Manual’s treatment of cyber operations is a useful indication of the current state of international law development in cyberspace and offers insights into likely future developments.

Despite presenting the opportunity to do so, it will be found that the Manual declines to resolve considerable and relatively long-standing legal questions.

---

8 Id. at 42-43, 75. In international law, the phrase ius ad bellum refers to the legal regime that governs states’ resort to force in their international relations. See Marco Sassòli, Antoine Bouvier, and Anne Quintin, How Does Law Protect in War? 114-15 (3d ed., 2011). The phrase ius in bello describes the legal regime that regulates the conduct of hostilities during armed conflict. Id.


concerning the operation of the law of war in cyberspace. Although they describe the US as committed to resolving unsettled and undeveloped legal issues in cyberspace, the Manual’s authors decline to employ it as a means to stake out meaningful positions with respect to these issues or to resolve them in any significant respect. The Manual, with minor exceptions, is not a significant contribution to the development or refinement of cyber law. It leaves the international legal community uncertain with respect to a number of substantive legal issues in cyberspace as well as to how, if at all, the US intends to develop the law of war applicable to cyberspace.

2. The Manual and International Cyber Norm Development

The US Law of War Manual reflects not only the most significant expression of US views on the law of war in nearly sixty years, it is also the most detailed, publicly available catalogue of US legal guidance on cyber operations since a legal assessment published by the DoD Office of General Counsel in 1999. Despite frequent references to compliance with international law in a variety of policy statements and cyber strategy documents, prior to the Manual’s release the DoD had not issued any publicly available and generally applicable legal guidance applicable to cyber operations since the 1999 assessment. And while the Legal Advisor to the US Department of State did offer highly-publicised (and closely studied) remarks on the application of international law to cyber operations at the founding of the US Cyber Command in 2012, his statements offered little in the way of specific doctrine or the operation of any particular aspect of the law of war.

At its outset, the Manual’s chapter on cyber operations notes enduring US efforts ‘to clarify how existing international law and norms … apply to cyber operations.’ In particular, the chapter cites US participation in a United Nations-led effort to secure state cooperation on international cyber and information security norms. This UN effort, namely the periodic meetings of a Group of Governmental Experts (GGE), has touted clarifying and developing the operation of international law

---

14 See e.g. Office of the White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, 9 (May 2011) affirming the application of international law to states’ operations and activities in cyberspace.
applicable to information and communications technology as a critical component of maintaining international peace and security.\textsuperscript{18} US participation reflects, according to the \textit{Manual}, an important policy-based commitment to the application and relevance of international law to cyber operations.\textsuperscript{19} As further evidence of interest in developing legal norms applicable to state behaviour in cyberspace, the \textit{Manual} cites a Department of Defense report to the US Congress which notes that the US is ‘actively engaged in the continuing development of norms’.\textsuperscript{20} Although it is possible that the report intends to refer to other efforts or to development of political norms, it is likely that the report’s reference to active engagement refers to US participation in the ongoing UN GGE process. The \textit{Manual} does not identify any other active processes of cyber law development.

Immediately following its avowal of the US commitment to international cyber law development, however, the \textit{Manual} includes an important qualification. Addressing the international law of war particularly, the \textit{Manual} notes that the law is ‘not well-settled, and aspects of the law in this area are likely to continue to develop’.\textsuperscript{21} While undoubtedly accurate with respect to a number of important law of war rules, this qualification may also be an important comment on the extent to which the US considers cyber operations conclusively regulated by international law. By characterising legal issues as unsettled or undeveloped, the \textit{Manual} may not be merely describing the state of the law as understood by DoD, it may also be signalling how the US expects to regulate cyber operations. That is, the instances the \textit{Manual} identifies as unclear or unsettled reflect not only substantive legal evaluations, but also reflect methodological judgments about the level and nature of commitment to international law which states must demonstrate to truly commit an activity in cyberspace to international regulation. At minimum, the observation confirms the US viewpoint that a number of important regulatory ambiguities and even voids exist under the current legal framework. How and, in particular, whether to fill these gaps are crucial questions.

The \textit{Manual}’s first substantive evaluation of how the law of war operates in cyberspace concerns a question of \textit{ratione materiae} or what cyber situations fall within the subject matter regulated by the law of war. The \textit{Manual} quickly dismisses the Exceptionalist view, observing that even rules developed before the advent of cyberspace are applicable to cyber operations.\textsuperscript{22} Nothing about the structure, composition or operation of cyberspace convinces the \textit{Manual}’s authors that cyberspace is a legal void or unregulated by existing law.

The same section on application notes ‘challenging legal questions’ owing to the wide range of effects, including non-kinetic effects, that cyber operations involve.

\textsuperscript{20} \textit{Id.} at 994, n. 1.
\textsuperscript{21} \textit{Id.} at para. 16.1.
\textsuperscript{22} \textit{Id.} at para. 16.2.1.
For instance, the Manual notes that cyber operations which merely involve information gathering may not implicate rules applicable to attacks. However the Manual refrains from offering any conclusive methodology, such as an effects-based approach, to resolving these questions.

In the following section, the Manual identifies, depending on how one tallies them, three or five principles of the ius in bello. The Manual states that ‘[t]hree interdependent principles – military necessity, humanity, and honor – provide the foundation for other law of war principles, such as proportionality and distinction, and most of the treaty and customary rules of the law of war.’ Addressing how these principles operate in cyberspace, the Manual notes significant ambiguity. Specifically, it indicates that cyber operations ‘may not have a clear kinetic parallel in terms of their capabilities and the effects they create.’ Although the Manual does not provide an example, cyber operations that merely alter or impede the functions of a target rather than destroy it come to mind. The exact extent to which such operations implicate the Manual’s law of war principles is therefore unclear. The Manual offers no methodology or legal conclusion that would guide future analyses with respect to these questions beyond advising its audience that ‘suffering, injury, or destruction unnecessary to accomplish a legitimate military purpose must be avoided.’

This observation suggests a role for at least one of the principles, that of military necessity, in cyber operations not clearly analogous to hostilities. But exactly which principles operate in such cases and how is left unclear.

In a departure from its nearly exclusive focus on ius in bello issues throughout, the Manual next addresses cyber operations and the ius ad bellum. With respect to the prohibition of the use of force, the Manual unsurprisingly confirms that cyber operations are capable of producing effects consistent with the use of force and therefore of amounting to violations of the prohibition. With respect to the ‘armed attack’ threshold that activates states’ right to use force in self-defence, the Manual observes that ‘any cyber operation that constitutes an illegal use of force against a state potentially gives rise to a right to take necessary and proportionate action in self-defense.’ Lawyers steeped in the ius ad bellum will recognise this very permissive characterisation of the right of self-defence as consistent with a long held US legal opinion that the ‘use of force’ and ‘armed attack’ are synonymous, an opinion that is controversial and has become increasingly isolated. While a contentious legal issue, the armed attack threshold question is certainly not unique to the cyber context and therefore unlikely

23 See e.g. Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts, arts 49-58, June 8, 1977, 1125 U.N.T.S. 3 enumerating rules and precautions that regulate ‘attacks’ as defined in Article 49 of the Protocol.
25 Id. at para. 16.2.2.
26 Id.
27 The first chapter of the Manual includes an orientation to the ius ad bellum. Id. at paras. 1.11-1.11.5.6.
28 Id. at para. 16.3.
29 US Law of War Manual, at para.16.3.3.1
30 See Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. US), 1986 I.C.J. 14, para. 191 (June 27) describing the ‘use of force’ and ‘armed attack’ as distinct legal standards with the latter reflecting more grave instances of the former.
to be resolved definitively as a purely cyber norm. Still, the Manual’s position equating the use of force with armed attack would seem to strengthen the need to clarify the use of force threshold with cyber examples or better yet an analytical model, an opportunity the Manual declines in significant part.

Importantly, the Manual indicates that questions concerning the legality of states’ use of force by cyber means, especially in response to other actors’ cyber operations, are greatly complicated by the difficulties of attribution.\(^{31}\) Cyberspace offers malicious actors considerable opportunities to maintain their anonymity or to spoof the identity of other actors or states. Strong disagreement exists whether international law imposes on victim states a duty to meet a standard of proof prior to exercising self-defence. Some international lawyers argue that, prior to taking action, a responding state must achieve a requisite degree of certainty as to attribution akin to meeting an evidentiary standard in litigation as part of the law of state responsibility.\(^{32}\) Others find inadequate support for the notion that states have committed anything of the sort to international law.\(^{33}\) For its part, the Manual makes no attempt to identify, clarify, or for that matter even reject the existence of any international legal standard with respect to attribution, or to develop a cyber norm regarding this issue.

Finally, with respect to its treatment of the \textit{ius ad bellum}, the Manual does not identify or discuss standards for attributing cyber operations by non-state actors to states. The significant cyber capabilities of non-state actors and the opportunity to evade attribution have induced many states to outsource their cyber operations to private groups.\(^{34}\) Still, the question of non-state actor attribution is not new or even unique to cyberspace. A number of judgments by international tribunals and courts have tackled the question, producing competing standards. Specifically addressing state responsibility, the International Court of Justice (ICJ) has held that to attribute to a state the action of a non-state group that is not an organ of that state, the state in question must exercise ‘effective control’ over the relevant act.\(^{35}\)


\(^{32}\) See e.g. Mary Ellen O’Connell, \textit{Evidence of Terror}, 7 Journal of Conflict and Security Law 22 (2002) arguing, outside the context of cyber operations, that invoking self-defence requires ‘clear and convincing evidence’. See also Marco Roscini, Cyber Operations and the Use of Force in International Law 98-99 (2014). Roscini appears to advocate the clear and convincing evidence standard based on litigation of state responsibility claims at the International Court of Justice. \textit{Id.}\ It is unclear whether Roscini regards the clear and convincing standard as applicable outside the context of ICJ litigation as a general prerequisite to lawful state exercise of self-defence. He appears to have softened his position in a recent publication; Marco Roscini, \textit{Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations}, 50 Texas International Law Journal 233, 250 (2015).


the relevant conduct of the group in question; general influence on or support for the group is not sufficient to establish attribution under the effective control standard.  

Since the ICJ announced its effective control standard, some have construed a less stringent standard – the ‘overall control’ standard used by the International Criminal Tribunal for Former Yugoslavia for purposes of applying the *ius in bello* – as a more appropriate standard for attribution, especially in cyberspace. Where the effective control standard requires the state in question directly influence the specific acts in question, the overall control standard merely requires that the state wield general influence over the group or non-state actor in question. Clearly, under the overall control standard more cyber actions by more non-state actors would be attributable to more states for purposes of state responsibility or remedial action by a victim state. The Manual’s decision to address the *ius ad bellum* without offering guidance as to the correct legal standard for attribution is surprising and leaves the debate somewhat unresolved. As a frequent victim of malicious cyber operations by non-state actors with alleged ties to rival states, it would seem DoD would be anxious to describe or to advocate an appropriate legal standard for attribution of such acts.

In an encouraging sign of awareness, the Manual includes treatment of the often neglected law of neutrality. Applicable during international armed conflict, the law of neutrality outlines duties and responsibilities of both states not party to the armed conflict in question as well as belligerent states. The law of neutrality has long regulated communications of belligerent parties routed through neutral territory. Generally speaking, belligerent states may not erect military communications infrastructure on neutral territory. However, the law of neutrality has historically permitted belligerent states to route communications through publicly available communications infrastructure located on neutral territory without imposing on neutral states any obligation to prevent such use.

The Manual applies this relatively permissive neutrality regime in significant part to cyber operations as well. It observes, ‘it would not be prohibited for a belligerent state to route information through cyber infrastructure in a neutral state that is open for the service of public messages …’ With some equivocation, the Manual surmises that even cyber communications that carry or deliver cyber weapons or that cause destruction in a belligerent state would not be prohibited. Although

---

39 Id. art. 3.
40 Id. art. 3(a).
41 Id. art. 3(b).
43 Id. observing ‘Thus, for example, it would not be prohibited for a belligerent state to route information through cyber infrastructure in a neutral state that is open for the service of public messages … This rule would appear to be applicable even if the information that is being routed through neutral communications infrastructure may be characterised as a cyber weapon.’
certainly a colourable interpretation of the law of neutrality, the conclusion is surprising in light of the general tenor of the law, which appears to prohibit the exercise of belligerent functions, such as attacks, through or from the territory of neutral states. Whether objectively correct or not, the Manual’s position seems precisely the sort of stance with respect to unclear or ambiguous law needed to contribute to the development of international cyber legal norms.

Consistent with the Manual’s general approach, the cyber operations chapter devotes the majority of its attention to the ius in bello. Appropriately, the first ius in bello issue it considers is the threshold of ‘attack’ in the context of cyber operations. In accordance with an apparent majority of international lawyers, the Manual reserves application of the ius in bello rules on targeting to operations that amount to an attack. To illustrate, the Manual cites a cyber operation ‘that would destroy enemy computer systems’ as prohibited if directed against civilian infrastructure. The Manual notes that rules that apply to attacks do not apply to operations below the attack threshold and such operations may therefore be directed, consistent with the law of war, against civilians or civilian objects subject to the requirement of military necessity. Examples of such operations include webpage defacement, disruption of Internet services, and dissemination of propaganda.

However, the Manual declines to identify comprehensive criteria or a detailed test for distinguishing cyber attacks from ordinary cyber operations. The Manual merely observes that cyber operations resulting only in reversible or temporary effects may not amount to an attack. A more thorough analysis or mode of scrutiny, such as that found in the Tallinn Manual, might have been offered (or for that matter might have been explicitly rejected) to clarify an effective international rule on the subject. Worse, the Manual significantly confuses the issue by observing, ‘A cyber operation that would not constitute an attack, but would nonetheless seize or destroy enemy property, would have to be imperatively demanded by the necessities of war’. It is unclear why the described operation is not an attack if it destroys enemy property, unless perhaps the relevant destruction is incidental rather than integral to the operation or is an uncontested operation during belligerent occupation pursuant to requisition or seizure.

Continuing its coverage of targeting considerations, the Manual’s treatment of required precautions against incidental harm to civilians and civilian objects is unsurprising and consistent with longstanding US legal doctrine. However, the section includes an important observation concerning the duty to take precautions and

---

44 See Hague Convention V, supra note 156, arts 2-5.
45 See e.g. Tallinn Manual, supra note 125, at 106-10.
47 Tallinn Manual, supra note 125, at 106-10 addressing in commentary considerations such as effects on functionality and the nature remedial measures required to reinstate functionality as factors relevant to identifying cyber attacks.
49 See Hague Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, arts 52 and 53, October 18, 1907, 36 Stat. 2277. The law of belligerent occupation anticipates and does not prohibit requisitions and seizures of some categories of enemy property. Seizure or requisition may result in lawful destruction of some property. Id.
victims of cyber attacks, noting that the requirement to take feasible steps to reduce incidental civilian injury and damage is not limited to attackers. The Manual observes that parties subject to attack must also take steps to reduce civilian harm in the event of attacks on their systems. Although the cyber operations chapter does not elaborate, a preceding chapter expands on defenders’ duties in this regard. The defenders’ duty seems especially important and a particularly effective means of reducing civilian harm resulting from hostile cyber operations given the prevailing dual, military-civilian nature and use of the Internet and much cyber infrastructure. This section could prove exceptionally important evidence of a critical international legal norm respecting network design and use by armed forces.

Respecting the principle of proportionality, and also the rule of proportionality related to precautions in attack, the Manual offers a useful, if contestable, observation concerning assessment of incidental damage. Generally speaking proportionality prohibits attacks expected to produce ‘loss of life or injury to civilians, and damage to civilian objects incidental to the attack’ that would be ‘excessive in relation to the concrete and direct military advantage expected to be gained’. The Manual excludes from the notion of incidental damage, and therefore from proportionality calculations, ‘mere inconveniences or temporary losses’ including ‘brief disruption of internet services to civilians’ as well as ‘economic harms in the belligerent state resulting from such disruptions’. As with the preceding observations concerning defenders’ duty to take precautions against harm to civilians, this observation is strong evidence of an influential state’s desire to express a legal norm refined to the context of cyberspace.

A paragraph on improper use of signs offers a flurry of examples of prohibited and permissible use of disguised cyber traffic. According to the Manual, the law of war prohibits cyber attacks ‘making use of communications that initiate non-hostile relations, such as prisoner exchanges or ceasefires’. In this regard the Manual offers helpful treatment of the question of deception that has proved critical to the success of a number of cyber operations.

The Manual addresses the issue of civilian participation in cyber operations as well. It notes neither a prohibition on civilian support to cyber operations of any sort, nor any prohibition on civilians’ direct participation in cyber hostilities. In support of the former view, the Manual notes the 1949 Third Geneva Convention provision according prisoner of war (POW) status to civilians accompanying armed forces, seemingly equating these civilians’ POW status with an international law

50 Id. para. 16.5.3.
51 Id. at para. 5.14.
52 See id. at para. 2.4.
53 See id. para. 5.12.
54 Id. See also AP I, supra note 24, art. 51(5)(b).
56 Id. at para. 16.5.4.
57 Id.
ratification of the legitimacy of their support to military operations.\textsuperscript{59} With respect to the latter, the \textit{Manual} simply notes that civilians taking direct part in cyber hostilities forfeit their protection for intentional attack by enemy forces.\textsuperscript{60} Although an earlier section of the \textit{Manual} includes detailed discussion of the notion of direct participation in hostilities, the chapter offers no elaboration on how the concept operates with respect to support to or conduct of cyber operations.\textsuperscript{61}

As a final \textit{ius in bello} matter, the cyber operations chapter considers issues associated with legal reviews of cyber weapons. The \textit{Manual} identifies the requirement to conduct legal reviews of new weapons as a requirement of DoD policy.\textsuperscript{62} Although an earlier chapter notes that Article 36 of Additional Protocol I to the 1949 Geneva Conventions requires state parties to conduct legal reviews of new weapons, the \textit{Manual} declines to indicate whether the US regards the requirement as reflective of customary international law as well.\textsuperscript{63}

The \textit{Manual} adds a degree of clarity to the weapons review requirement by noting that ‘[n]ot all cyber capabilities, however, constitute a weapon or weapons system.’ Yet it offers no standard by which such distinctions between cyber weapons and other code might be made. Moreover, the \textit{Manual} declines to weigh in on whether mere alterations to existing cyber weapons are either permissible or require new legal reviews. The \textit{Manual} appears to leave such questions to the various services of the DoD. The question is important given the mutable nature of cyber weapons and the fact that the most sophisticated cyber weapons often require frequent, even real time adjustments to ensure their effectiveness. The \textit{Manual} might have offered significant clarification in this respect, both to its community of lawyers and to the international legal community.

3. Reflections on the Future of Cyber Norm Development

As an indication of a major power’s willingness to submit to meaningful international regulation of its cyber operations, especially during armed conflict, the \textit{Manual} offers mixed signals. On one hand, the \textit{Manual} includes a number of statements that suggest strong US interest in refining and clarifying norms applicable to states’ cyber operations. These observations and seeming commitments offer hope to those interested in resorting to international law and norms to regulate cyberspace. Moreover, the \textit{Manual}'s cyber operations chapter is a resounding rejection of the

\textsuperscript{59} US Law of War Manual, \textit{supra} note 10, at para. 16.5.5.
\textsuperscript{60} \textit{Id.}
\textsuperscript{61} \textit{Id.} at para. 5.9.
Exceptionalist view on the relationship between international law and cyberspace. The *Manual* unequivocally regards existing international law as a source of binding norms on states’ conduct of cyber operations.

To a limited extent and on limited subjects, the *Manual* also follows up on US purported commitment to further cyber law development and refinement. The *Manual*’s sections on neutrality, proportionality, and precautions against civilian harm offer constructive guidance and seeming *opinio juris* on important ambiguities. Each section offers simultaneously clear expressions of applicable legal standards and useful illustrations of how those standards are understood to operate with respect to modern cyber operations.

On the other hand, the *Manual* does little of its own accord to resolve many of the unsettled and developing provisions it notes as problematic. For instance, the *Manual* resists adopting a specific analytical methodology for sorting the legal significance of cyber operations that produce effects short of destruction or violence. The *Manual* might, in relatively short order, have announced a clear position with respect to what particular cyber operations or consequences thereof relate to the *ratione materiae* of the law of war.

Similarly, the *Manual* might have staked out a clear position on the vexing issue of attribution of non-state actors’ conduct to states for purposes of state responsibility, in particular for the exercise of countermeasures or self-defence. In light of the competing effective control and overall control standards, the *Manual* might have weighed in to sway, if not resolve, lingering debate on a crucial cyber norm.

The *Manual* also declines to flesh out a coherent conception of the use of force with respect to cyber operations. A quite comprehensive and systematic approach to evaluating cyber operations under the use of force standard has circulated for quite some time now and has attracted significant support. That the *Manual* declines to comment in support of or against that model, is curious given the decision to address the *ius ad bellum* both generally and specifically with respect to cyber operations.

Perhaps if the *Manual* is understood to be a work primarily concerned with the *ius in bello*, the preceding decisions with respect to *ius ad bellum* and state responsibility law might be understandable. Less understandable, however, is the decision to decline to contribute normative viewpoints on a number of *ius in bello* issues relevant to cyber operations. The *Manual*’s thin treatment of the attack threshold for applying targeting rules, direct participation in cyber hostilities, and the extent and nature of the requirement to review cyber weapons reflects a clear decision not to weigh in significantly on subjects that will appear to many to be suitable for development of cyber-specific legal norms.

It is difficult to imagine the *Manual*’s authors were unaware of these unresolved issues presented by cyber operations. Its authors and reviewers, including members

---

of the US DoD Law of War Working Group, are exceptionally well-informed of the
current legal challenges of the cyber domain. And presented with the ambiguities
identified by the Tallinn Manual, the DoD Manual faced a somewhat easier task of
identifying topics the international legal community regarded as ripe for clarifica-
tion. The DoD Manual might easily have commented favourably or otherwise on
any number of the various competing majority and minority views offered by the
Tallinn group members.

There are a number of possible explanations for the Manual’s limited contri-
butions to interpretive clarity. The first relates to methodology. In its introdutory
chapter, the Manual explains that it is not intended as a definitive work on US law
of war opinio juris.65 While understandable, especially considering the diffusion of
responsibility within the US Government for managing its relationship to interna-
tional law, the expectation that the international community will read the Manual
as something other than an expression of opinio juris may be naive or even unreas-
sonable.

A second explanation relates to timing. It is certainly possible that the Manual’s
sparse legal refinements reflect a determination on the part of DoD that commitment
to developed norms in cyberspace would simply be premature. The Manual incorpo-
rates by reference an observation to this effect in an early footnote, observing:

‘The international community ordinarily does not negotiate treaties to deal
with problems until their consequences have begun to be felt. This is not
all bad, since the solution can be tailored to the actual problems that have
occurred, rather than to a range of hypothetical possibilities. One conse-
quence, however, is that the resulting law, whether domestic or international,
may be sharply influenced by the nature of the events that precipitate legal
developments, together with all their attendant policy and political consid-
erations. … Similarly, we can make some educated guesses as to how the
international legal system will respond to information operations, but the
direction that response actually ends up taking may depend a great deal on
the nature of the events that draw the nations’ attention to the issue. If inform-
action operations techniques are seen as just another new technology that
does not greatly threaten the nations’ interests, no dramatic legal develop-
ments may occur. If they are seen as a revolutionary threat to the security
of nations and the welfare of their citizens, it will be much more likely that
efforts will be made to restrict or prohibit information operations by legal
means. These are considerations that national leaders should understand in
making decisions on using information operations techniques in the current
formative period, but it should also be understood that the course of future
events is often beyond the control of statesmen.’66

66 Id. at 995, n. 2.
The statement reflects an undoubtedly accurate observation of the development of international legal norms in newly emerged areas of state interaction. However, the statement was originally made with respect to cyber operations in 1999. If it is true that the community of states ‘does not negotiate treaties to deal with problems until their consequences have begun to be felt,’ then it may be fair to question whether the problems of cyber operations remain unfelt by states fifteen years later. If uncertainties with respect to cyber operations are sufficient to prevent states from achieving legislative consensus persist and the Manual also evades addressing them, it seems likely that DoD regards them as still not ripe for development or resolution. That is, it may be the view of the General Counsel that activities in cyberspace should be permitted to continue to play out under these legal ambiguities before committing to clearer norms.

A third and highly pragmatic explanation relates to security classification. Although a great deal of information has been released publicly, the details of most states’ cyber operations, capabilities and tactics remain highly classified. It is entirely possible that while the Manual’s authors held and have perhaps even issued detailed guidance concerning the law of war and cyber operations, these views could not be published publicly without compromising highly sensitive information. Precedent for this approach can be found among US legal opinions issued with respect to detention operations early during the military campaigns that followed the attacks of September 11, 2001. These highly controversial but also highly detailed and exhaustively reasoned opinions were held at extraordinarily high levels of security classification and were not released, but rather were leaked. It is not difficult to imagine that similarly detailed analyses, including clear positions on a number of legal norms, exist today in highly classified US Government legal opinions.

To be clear, none of these aspects of the Manual necessarily reflects shortcomings or failings. I do not wish in any respect to suggest the Manual or the US is under any duty or has the capacity to unilaterally clarify or perfect the international law applicable to cyber operations. There are doubtless a great number of assumptions behind the Manual’s cyber chapter. Chief among them may be that the law of war applicable to cyber operations leaves many issues unresolved and therefore in some respects unregulated, and that this is often desirable. The Manual may simply be evidence that ambiguity from the perspective of the US is appropriate with respect to any number of legal voids.

Given the Manual’s enormous size, analysis and critiques have been understandably slow to emerge. A fair assessment must, however, conclude that its authors

67 Legal Issues in Information Operations, supra note 131.
68 See generally The Torture Papers (Karen J. Greenberg and Joshua L. Dratel, eds., 2005) compiling leaked classified memos concerning detention practices of the executive branch during early stages of the Global War on Terrorism.
were neither negligent nor evasive. What the *Manual* clarifies with respect to cyber operations and what it leaves unresolved should be understood simply as a snapshot of the state of international law cyber norms as well as an indication of a single state's limited interest in immediately cultivating more developed and meaningful international norms in that area. More than simply confirmation of persistent ambiguities in the operation of the law of war in cyberspace, the ambiguities the *Manual* leaves unresolved are strong evidence of the US' comfort with these uncertainties and legal voids. Alongside the halting and fitful UN GGE process for development of international cyber norms, the *Manual* indicates significant state reticence toward and even a present inclination against definitive clarity and precision in this challenging domain of state competition.