International Cyber Norms:
Legal, Policy & Industry Perspectives,
Anna-Maria Osula and Henry Rõigas (Eds.),
NATO CCD COE Publications, Tallinn 2016

CHAPTER 3

Cyber Law Development and the United States Law of War Manual

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]

1 John Perry Barlow, *A Declaration of the Independence of Cyberspace*, Electronic Frontier Foundation, (1996) accessed July 11, 2015, https://projects.eff.org/~barlow/Declaration-Final.html. *See also* David R. Johnson and David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 Stanford Law Review 1367 (1996).

2 Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 Georgetown Law Journal 317, 326 (2015).

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.[3] Scholars sometimes refer in this respect to a 'cybered Westphalian age'.[4]

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.[5] 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.[6] 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.[7]

3 *See* Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 Indiana Journal of Global Legal Studies 475 (1998) [hereinafter Goldsmith].

4 Joanna Kulesza and Roy Balleste, *Signs and Portents in Cyberspace: The Rise of* Jus Internet *as a New Order in International Law*, 23 Fordham Intellectual Property, Media and Entertainment Law Journal 1311, 1319-20; citing Chris C. Demchak and Peter Dombrowski, *Rise of a Cybered Westphalian Age*, Strategic Studies Quarterly, Spring 2011, at 32, 32. For descriptions of a similar concept see Duncan B. Hollis, *Rethinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, *in* Jens Ohlin, Kevin Govern, and Claire Finklestein eds., 2015 Cyberwar: Law & Ethics for Virtual Conflicts 133-34.

5 *See* Jack L. Goldsmith and Tim Wu, Who Controls the Internet? Illusions of a Borderless World (2008); Goldsmith, *supra* note 121, at 476.

6 *See* Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law* Opinio Juris *and the Law of Cyber Warfare*, 50 Texas International Law Journal 189 (2015) criticizing states' reluctance to participate in international law formation through expressions of legal opinions.

7 Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013) (hereinafter Tallinn Manual). The present author was a member of the International Group of Experts that produced the *Tallinn Manual*.

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*.[8]

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.[9]

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*[10] (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.*

9 *See e.g.* Priyanka R. Dev, *'Use of Force' and 'Armed Attack' Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response*, 50 Texas International Law Journal 381, 397-400 (2015) noting legal deficiencies in cyber law as characterised by the *Tallinn Manual* and advocating refinement of legal thresholds.

10 US Department of Defense, Office of the General Counsel, Law of War Manual (2015), accessed July 27, 2015, http://www.defense.gov/pubs/Law-of-War-Manual-June-2015.pdf (hereinafter US Law of War Manual).

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,[11] 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,[12] 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.[13] 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.[14] 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.[15]

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'.[16] In particular, the chapter cites US participation in a United Nations-led effort to secure state cooperation on international cyber and information security norms.[17] This UN effort, namely the periodic meetings of a Group of Governmental Experts (GGE), has touted clarifying and developing the operation of international law

11 US Law of War Manual, para. 16.1.

12 The *Manual*'s predecessor, *The Law of Land Warfare*, was published in 1956 and, with the exception of a minor 1976 addendum, served unaltered as the primary law-of-war resource of US Department of Defense lawyers until 2015. *See* US Dep't of the Army, the Law of Land Warfare, Field Manual 27–10 (July 1956).

13 US Dep't of Defense, Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (November 1999), *reprinted in* 76 International Law Studies 459 (2002) (hereinafter *Legal Issues in Information Operations*).

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.

15 US Department of State, Legal Advisor, Harold Hongju Koh, *International Law in Cyberspace*, (September 18, 2012), accessed 27 July 2015, http://www.state.gov/s/l/releases/remarks/197924.htm.

16 US Law of War Manual, *supra* note 128, para. 16.1.

17 United Nations Office for Disarmament Affairs, *Developments in the Field of Information and Telecommunications in the Context of International Security*, accessed July 27, 2015, http://www.un.org/disarmament/topics/informationsecurity.

applicable to information and communications technology as a critical component of maintaining international peace and security.[18] US participation reflects, according to the *Manual*, an important policy-based commitment to the application and relevance of international law to cyber operations.[19] As further evidence of interest in developing legal norms applicable to state behaviour in cyberspace, the *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'.[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 *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 *Manual* includes an important qualification. Addressing the international law of war particularly, the *Manual* notes that the law is 'not well-settled, and aspects of the law in this area are likely to continue to develop'.[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 *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 *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 *Manual*'s first substantive evaluation of how the law of war operates in cyberspace concerns a question of *ratione materiae* or what cyber situations fall within the subject matter regulated by the law of war. The *Manual* quickly dismisses the Exceptionalist view, observing that even rules developed before the advent of cyberspace are applicable to cyber operations.[22] Nothing about the structure, composition or operation of cyberspace convinces the *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.

18 U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/172, (22 July 2015); G.A. Res. 69/28, para. 4, U.N. Doc. A/RES/69/28 (Dec. 11, 2014).
19 US Law of War Manual, *supra* note 10, at para. 16.1.
20 *Id*. at 994, n. 1.
21 *Id.* at para. 16.1.
22 *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.[23] 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'.[24] 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'.[25] 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'.[26] 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*.[27] 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.[28] 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'.[29] 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.[30] 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.

24 US Law of War Manual, *supra* note 10, para. 2.1.

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 *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] Importantly, the effective control standard is understood to require the state to exert direct influence on

31 US Law of War Manual, *supra* note 10, at para. 16.3.3.4. *See e.g.* Choe Sang-Hun, *North Korea denies Role in Sony Pictures Hack*, New York Times, Dec. 7, 2014, http://www.nytimes.com/2014/12/08/business/north-korea-denies-hacking-sony-but-calls-attack-a-righteous-deed.html?action=click&contentCollection=Asia%20Pacific&module=RelatedCoverage&region=Marginalia&pgtype=article describing difficulty attributing 2014 hack of Sony Pictures systems.

32 *See e.g.* Mary Ellen O'Connell, *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. *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, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, 50 Texas International Law Journal 233, 250 (2015).

33 *See* Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, 56 Villanova Law Review 569, 595 (2011) acknowledging the clear and convincing standard but resorting primarily to a general requirement of reasonableness. The *Tallinn Manual* does not include a rule identifying evidentiary standards as prerequisites to state responses.

34 *See e.g.* Michael Riley and Jordan Robertson, *Chinese State-Sponsored Hackers Suspected in Anthem Attack*, Bloomberg Business, Feb. 5, 2015, http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack describing alleged relationships between private computer hacking groups and the Chinese government.

35 Paramilitary Activities, paras. 116-17. *See also* Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz v. Serbia & Montenegro), 1996 I.C.J. 595, para. (July 11) reaffirming the Court's effective control test.

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.[36]

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.[37] 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.[38] The law of neutrality has long regulated communications of belligerent parties routed through neutral territory.[39] Generally speaking, belligerent states may not erect military communications infrastructure on neutral territory.[40] 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.[41]

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 … '. [42] 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.[43] Although

36 *See* Nicholas Tsagourias, *Cyber Attacks, Self Defence and the Problem of Attribution*, 17 Journal of Conflict and Security Law 229, 238 (2012).

37 *See Prosecutor v. Tadić*, Case No. IT-94-1-A, Appeals Chamber Judgment paras. 131, 145 (Intl'l Crim. Trib. for the Former Yugoslavia July 15, 1999). *See* Scott J. Shackelford, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, *in* Conference on Cyber Conflict Proceedings 2010 (Christian Czosseck and Karlis Podins eds., 2010) advocating use of the overall control standard for attribution of state responsibility in the cyber context.

38 *See generally* Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct.18, 1907, 36 Stat. 2310 (hereinafter Hague Convention V).

39 *Id.* art. 3.

40 *Id.* art. 3(a).

41 *Id.* art. 3(b).

42 US Law of War Manual, *supra* note 10, at para. 16.4.1.

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.[44] 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.[45] 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.[46] 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.[47] 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'.[48] 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.[49]

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.
46 US Law of War Manual, *supra* note 10, at para. 16.5.2.
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.
48 US Law of War Manual, *supra* note 10, at para. 16.5.1.
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.[50] 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.[51] 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,[52] and also the rule of proportionality related to precautions in attack,[53] 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'.[54] 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'.[55] 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.[56] 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'.[57] 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,[58] 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).
55 US Law of War Manual, *supra* note 10, at para. 16.5.1.1.
56 *Id.* at para. 16.5.4.
57 *Id.*
58 Geneva Convention (III) Relative to the Treatment of Prisoners of War, art. 4A(4) August 12, 1949, 75 U.N.T.S. 135.

ratification of the legitimacy of their support to military operations.[59] With respect to the latter, the *Manual* simply notes that civilians taking direct part in cyber hostilities forfeit their protection for intentional attack by enemy forces.[60] Although an earlier section of the *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.[61]

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

The *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 *Manual* declines to weigh in on whether mere alterations to existing cyber weapons are either permissible or require new legal reviews. The *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 *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 *Manual* offers mixed signals. On one hand, the *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 *Manual*'s cyber operations chapter is a resounding rejection of the

59 US Law of War Manual, *supra* note 10, at para. 16.5.5.
60 *Id.*
61 *Id.* at para. 5.9.
62 *Id.* at para. 16.6 citing US Dep't of Defense, Directive 5000.01, *The Defense Acquisition System*, para. E1.1.15 (May 15, 2003).
63 US Law of War Manual, *supra* note 10, at paras. 6.2.3, 16.6.

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.[64] 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

64 Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Columbia Journal of Transnational Law 885 (1999) outlining a multi-criteria mode of analysis for evaluating cyber operations as use of force.

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 clarification. 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 contributions to interpretive clarity. The first relates to methodology. In its introductory 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 international 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 unreasonable.

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* incorporates 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 consequence, 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 considerations. … 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 information operations techniques are seen as just another new technology that does not greatly threaten the nations' interests, no dramatic legal developments 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]

65 US Law of War Manual, *supra* note 10, at para. 1.1.1.
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.[67] 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.[68] 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.[69] 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.

69 The webblog *Just Security* convened a 'mini forum' of initial reactions to the *Manual* during the summer of 2015. *See e.g.* Gary Brown, *Cyber Conflict in DOD's Law of War Manual*, Just Security (Jul. 27 2015), https://www.justsecurity.org/24950/cyber-conflict-dods-law-war-manual/; Geoffrey S. Corn, *Precautions to Minimize Civilian Harm are a Fundamental Principle of the Law of War*, Just Security (Jul. 8, 2015), https://www.justsecurity.org/24493/obligation-precautions-fundamental-principle-law-war/; Eric Jensen, *Law of War Manual: Information or Authoritative Guidance?*, Just Security (Jul. 1, 2015), https://www.justsecurity.org/24332/law-war-manual-information-authoritative-guidance.

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.