The Sony and OPM Double Whammy: International Law and Cyber Attacks

Tim McCormack

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

Recommended Citation
The Sony and OPM Double Whammy: International Law and Cyber “Attacks”

Tim McCormack*

I. CHARACTERIZING CYBER “ATTACKS”

One reality of dramatically increasing electronic connectivity is a commensurate increase in vulnerability to disruption. Computer network attacks are now so ubiquitous that they have become a hallmark of 21st century digital life. Reports suggest that, in 2014 alone, in excess of 317 million new pieces of malware were produced and released—a figure that translates into a staggering nearly one million new pieces of malware created on average every single day of the year. The trouble lies in the fact that software is fundamental to electronic functionality, and yet software is exceedingly difficult to produce without flaw. Exploitation of flaws in software via a release of targeted malware is not only commonplace but increasingly innovative, sophisticated, and audacious.

Fortune magazine claimed that the 2014 hack of Sony Pictures “terrified corporate America” and devastated the company—particularly with the loss of massive amounts of sensitive company data, including details of unreleased movies. The devastation’s extent exposed significant vulnerabilities in the corporation’s hardware (the malware destroyed the functionality of most of Sony’s desktops and laptops) and its data. Much of the compromised

* Tim McCormack is a Professor of Law at Melbourne Law School, an Adjunct Professor of Law at the University of Tasmania Law School and Special Adviser on International Humanitarian Law to the Prosecutor of the International Criminal Court in The Hague. He is currently a Fulbright Senior Scholar, Charles H. Stockton Distinguished Scholar-in-Residence at the Stockton Center for the Study of International Law at the U.S. Naval War College in Newport, Rhode Island, and James Barr Ames Visiting Professor at Harvard Law School. He is also a member of the international group of experts for Tallinn 2.0—the follow-up Manual on the International Law Applicable to Cyber Operations. The research for this article was supported under the Australian Research Council’s Discovery Projects funding scheme (project no. DP130100432). The author wishes to thank the editors of the SMU Science and Technology Law Review for the invitation to participate in their Symposium on Cyber Security. This article is a revised version of the paper the author presented at the Symposium in Dallas in October 2015.


2. Id. at 9.

3. Id.

4. See id.

data included sensitive personal identification details of Sony’s employees and personal e-mails of Sony management. The more recent hack of the U.S. Office of Personnel Management (OPM) resulted in the colossal theft of sensitive personal information of an estimated 21.5 million U.S. government employees—including Social Security numbers, security clearance application records, and digital fingerprint records. Anecdotal evidence suggests that some of the stolen data has already been sold and used for attempted identity fraud. Both Sony and the OPM are currently threatened with lawsuits, in the case of the OPM, by federal unions and disgruntled current and former U.S. government employees. The Office understands now, if it did not already, just how disgruntled victims of data theft can be.

Expressions of outrage were understandably common responses to both the Sony and the OPM hacks. Business Insider quoted Dave Aitel, former NSA research scientist and current CEO of Immunity, a cybersecurity firm, who characterized the Sony hack as an “act of war” and called for a reassessment on just how serious cyber attacks really are for U.S. national security. Similarly, Noah Rothman, writing for Commentary, chose to characterize the OPM hack as the nation’s “cyber Pearl Harbor” because, he claimed, the


hack was aimed at the "preventative neutering of America's defensive capabilities."\textsuperscript{12}

Claims such as these are not the exclusive domain of public commentators. Democratically elected politicians, ever conscious of answering to their electorates, have seized upon this terminology and forcefully argued that the United States is subject to a new form of warfare that demands a robust response. Senator John McCain of Arizona, for example, disagreed with President Obama's characterization of the Sony hack as "an act of cyber-vandalism that was very costly, very expensive."\textsuperscript{13} Senator McCain claimed on CNN's \textit{State of the Union} Program that

\begin{quote}
[t]he president does not understand that this is a manifestation of a new form of warfare... When you destroy economies, when you are able to impose censorship on the world and especially the United States of America, it's more than vandalism. It's a new form of warfare that we're involved in, and we need to react and react vigorously.\textsuperscript{14}
\end{quote}

Representative Carolyn Maloney of New York, in the context of a congressional hearing following the OPM hack, claimed that she considered this "attack... a far more serious one to the national security of our country"\textsuperscript{15} than the attacks of 9/11 because of the scale of the hack and the apparently coordinated effort to steal specific and comprehensive personal information on millions of key employees of the U.S. government.\textsuperscript{16}

Of course, others, including public commentators, academics, and elected decision-makers, have disavowed these characterizations of the hacks and argued that, while serious, even devastating, these hacks amount neither to acts of war nor to anything approximating a "cyber Pearl Harbor" or a "cyber 9/11."\textsuperscript{17}

\begin{itemize}
\item \textsuperscript{12}Noah Rothman, \textit{The Terrible Scale of the Chinese Cyber-Pearl Harbor Attack}, \textit{Commentary} (June 12, 2015), https://www.commentarymagazine.com/foreign-policy/asia/cyber-pearl-harbor-gets-worse/.
\item \textsuperscript{13}Kate Sheppard, \textit{McCain Calls Sony Hack an 'Act of War'}, \textit{Huffington Post} (Dec. 21, 2014, 11:16 AM), http://www.huffingtonpost.com/2014/12/21/sony-north-korea-war_n_6362454.html?.
\item \textsuperscript{14}Id.
\item \textsuperscript{16}U.S. Rep. Matt Cartwright Questions KeyPoint CEO Regarding the OPM Data Breach, \textit{YouTUBE} (June 24, 2015), https://www.youtube.com/watch?v=QacBhkKSkPSI.
\item \textsuperscript{17}See, e.g., Eichensehr, supra note 15; Henry Farrell, \textit{The Hack on the U.S. Government Was Not a 'Cyber Pearl Harbor' (But It Was a Very Big Deal)}, \textit{Wash. Post} (June 15, 2015), https://www.washingtonpost.com/blogs/monkey-cage/
While the debate on terminology and appropriate characterization rages, several areas of common ground have emerged. It is widely accepted that cyber attacks could be significantly more damaging, that the United States is vulnerable to devastating cyber attacks and that more must be done to secure computer networks and critical cyber infrastructure from future potential devastation. Temporary denial of online service is inconvenient, defacement of websites is embarrassing, and the theft of data may well be damaging. But future attacks could potentially disrupt public infrastructure with catastrophic consequences by interfering with air traffic control systems; shutting down public transport networks; disrupting emergency services; overriding controls for hydroelectric dams or nuclear power generation plants; or cutting off national or regional power supplies. Given the increasing sophistication of virtual attacks, it is presumably only a matter of time before those individuals intent on wreaking havoc use cyberspace as the operational theatre of choice. Additionally, there is a broad thirst for clarity on the proper characterization of hacks like those against Sony and OPM. Do these attacks constitute acts of war, acts of terrorism, crimes on a very large scale, vandalism, or all of the above? What are legitimate responses to attacks of this kind? What is and is not a permitted response? And of the permitted responses, which of them might constitute the most effective policy response?

For international lawyers, much of the popular debate, including choice of terminology in the characterization of the operations directed against the United States, evokes disquiet and frustration. The prevalence of the term "attack" to describe a cyber operation is a classic example. The popular use of the term is entirely understandable, and yet "attack" is a legal term of art with significant, potentially profound, legal and policy ramifications.

My intention is to focus on the relevant international legal concepts and to identify and discuss some of the ramifications arising from an international


19. See Holger Stark, Mossad’s Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War, SPIEGEL (Aug. 8 2011, 3:04 PM), http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html. The Stuxnet virus, used to attack the Iranian nuclear program, has been described as the most sophisticated computer virus ever developed, because it was designed to specifically target a particular program and to infect a “secure” computer system unconnected to the Internet. Id.
legal analysis of cyber operations of the kind experienced by SONY and OPM. Thus, although cyber defensive strategies to improve security against future cyber operations targeting critical infrastructure or the types of responses permitted by international law to hacks of this kind are clearly important issues that deserve greater attention, this article has a different focus.

II. THE TALLINN MANUAL ON CYBER WARFARE

The international group of experts responsible for the drafting of the Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) has already undertaken comprehensive analysis of the international legal issues relevant to the Sony and OPM hacks.20 The initiative to draft the Tallinn Manual was unusual because proactive clarification of applicable international law rarely occurs. The making of new, or even the clarification of existing, international law has tended to be reactive, often requiring a major catalyst to expose the need for either clarification or regulation. It has been rare in the history of international law for new development to preempt potential subsequent catastrophe. The initiative to draft the Tallinn Manual should, therefore, be warmly welcomed.

The authors of the Tallinn Manual, working under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia, recognized the potential for cyber warfare with devastating consequences for the victims of attacks and opted not to wait until such events occur before undertaking proactive clarification of the applicable law.21 It would be disingenuous, however, to imply that there was no reactive element in the drafting of the Tallinn Manual. The preparation of the Tallinn Manual under the auspices of the NATO CCD COE was not coincidental. The NATO Centre was established as a reaction to a major denial of service cyber operation against Estonia in 2007.22 Eneken Tikk, Kadri Kaska, and Liis Vihul have provided a comprehensive analysis of the nature of those cyber operations and, particularly, the distinct phases of the operations, manifest not only by ebbs and flows in the intensity and scale, but also in the level of coordination and the sophistication of the operations.23 This catalyst for the establishment of the NATO Centre also led NATO members to recognize the potential for cyber warfare with devastating consequences, and so the

authors of the *Tallinn Manual* have been proactively encouraged and supported to clarify the applicable law.

The original *Tallinn Manual*, published in 2013, includes two parts: Part A dealing with cyber security and the *jus ad bellum* (or the International Law on the Use of Force), and Part B with the *jus in bello* (also known as the Law of Armed Conflict (LOAC) or International Humanitarian Law). Since the publication of *Tallinn Manual* 1.0, a second international group of experts has convened to work on *Tallinn Manual* 2.0, a second volume of the manual to identify other international law applicable to cyber operations, such as, for example, the law of sovereignty, jurisdiction, international human rights law, diplomatic law, the law of State (and of international organization) responsibility, air law, space law, law of the sea, and the law of peace operations below the threshold of the law applicable to force.

The basic approach of the international group of experts for *Tallinn Manual* 1.0 (the international group of experts for *Tallinn Manual* 2.0 has adopted the same approach) was that relevant rules of conventional (treaty-based) and customary international law apply as much to cyber operations as they do to physical (or non-virtual) conduct. In other words, there is nothing specific to the means of conducting the activity that precludes the application of international law. This approach has been adopted notwithstanding the *Tallinn Manual*’s acknowledgement that “at the time the current international legal norms (whether customary or treaty-based) emerged, cyber technology was not on the horizon. Consequently, there is a risk that cyber practice [by states] may quickly outdistance agreed understandings as to its governing legal regime.”

The *Tallinn Manual* identifies two extreme positions: the first is consistent with the International Court of Justice (ICJ) position in the *Nuclear Weapons Advisory Opinion* and states that the law of armed conflict applies “to any use of force regardless of the weapons employed”; the second position applies the Permanent Court of Justice’s dictum in the *Lotus Case* explaining that acts not prohibited by international law are generally permitted. None of the members of the international group of experts has adopted the latter view and, as the *Tallinn Manual* asserts, the former app-

26. *See id.*
proach conforms to the views of both the International Committee of Red Cross (ICRC)31 and the U.S. government.32 The U.S. Department of Defense has reaffirmed the President’s approach in the 2014 Strategy for Cyberspace and cited the U.S. submission to a U.N. group of governmental experts, which the submission acknowledged had already accepted that general rules of international law apply to activities in cyberspace:

But the challenge is not whether existing international law applies to State behavior in cyberspace. As the 2012-13 GGE affirmed, international law does apply, and such law is essential to regulating State conduct in this domain. The challenge is providing decision-makers with considerations that may be taken into account when determining how existing international law applies to cyber activities. Despite this challenge, history has shown that States, through consultation and cooperation, have repeatedly and successfully applied existing bodies of law to new technologies. It continues to be the US view that all States will benefit from a stable international ICT [information and communication technologies] environment in which existing international law is the foundation for responsible State behavior in cyberspace.33

Adopting the position that international law applies just as much to cyber operations as to any other type of operations is not tantamount to arguing that the existing international legal framework is entirely capable of regulating all cyber operations. The Tallinn Manual emphasizes this point. However, the general approach of the Tallinn Manual’s international group of experts and also of states and international organizations certainly facilitates identification of the relevant legal framework applicable to attacks such as those experienced by Sony and the OPM.

The Tallinn Manual is not a source of law and does not represent the position either of NATO, any state, or any other organization. Instead the authors of the Tallinn Manual insist that it “be understood as an expression solely of the opinions of the [i]nternational [g]roup of [e]xperts, all acting in their personal capacity.”34 The Tallinn Manual adopts the orthodox premise

34. Tallinn Manual, supra note 20, at 11.
that international law regulates the use of force in two key respects.\textsuperscript{35} The \textit{jus ad bellum} regulates the circumstances in which states are permitted to resort to force.\textsuperscript{36} This body of international law imposes a general prohibition on use of force while allowing notable exceptions, principally force in national self-defense or under the auspices of U.N. Security Council approval.\textsuperscript{37} The \textit{jus in bello} applies to situations of armed conflict irrespective of compliance with the \textit{jus ad bellum} by any or all of the parties to the conflict.\textsuperscript{38} The \textit{jus in bello} regulates the conduct of hostilities, including the law of targeting, and imposes minimum standards of treatment for various categories of victims of armed conflict.\textsuperscript{39}

Both of these bodies of law, the \textit{jus ad bellum} and the \textit{jus in bello}, incorporate notions of "attack" with different legal ramifications arising from the respective contexts whenever the respective elements of an "attack" are satisfied.\textsuperscript{40} The \textit{Tallinn Manual} covers these areas of international law as they relate to cyber operations, and this article will also consider each in turn.

A. The \textit{Jus ad Bellum} and Cyber Operations

The primary reference to the term "attack" in the context of the \textit{jus ad bellum} arises in relation to a key exception to the general prohibition against resort to force. An "armed attack" is the critical prerequisite for legitimate resort to military force in self-defense by States acting individually (in defense of themselves) or collectively (in defense of another State).\textsuperscript{41} The right of national self-defense is recognized in Article 51 of the U.N. Charter which states, in relevant part, that: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."\textsuperscript{42}

Article 51 is an important provision, because it is one of only two explicit exceptions in the Charter to the general prohibition on resort to force.\textsuperscript{43}
Article 2(4) of the U.N. Charter imposes a treaty obligation that “[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”

The critical questions here are: (1) what conduct constitutes a threat or use of force falling within the scope of the prohibition in Article 2(4); (2) what conduct constitutes an “armed attack” triggering resort to force in legitimate self-defense; and (3) what is the relationship between prohibited “force” and an “armed attack”? Are they equivalent or is there a difference between them?

In relation to the first question—what conduct constitutes “force” prohibited by Article 2(4)—the Charter text offers no explanation. It is well known from the historical development of the prohibition on the use of force, as well as from the travaux préparatoires to Article 2(4), that the wording of the provision was intended to cover all resorts to military force. The motivation for such breadth in scope was to overcome the limitations of earlier prohibitions on resort to war as an instrument of national policy. The intention was not an absolute prohibition on resort to military force but a presumptive prohibition, subject to certain exceptions enumerated elsewhere in the Charter. The U.N. drafters agreed that the scope of the prohibition did not extend to economic and political force and, as the Tallinn Manual explains, this exclusion was reaffirmed in the drafting of the U.N. General Assembly’s 1970 Declaration on Friendly Relations.
The ICJ in the *Nicaragua* case provided helpful jurisprudence on the scope of the prohibition on the use of force. The court found, for example, that the laying of mines in Nicaragua's internal or territorial waters and attacks on Nicaraguan ports, installations, and a naval base all constituted force covered by the prohibition and were therefore unlawful unless subject to an exception. Direct intervention with kinetic force, such as the laying of naval mines and the perpetration of kinetic attacks against certain facilities and installations, unquestionably constitutes force within the scope of the prohibition. Perhaps the more interesting jurisprudence was the court's demarcation of types of indirect intervention by the United States in Nicaragua in the form of assistance to the *contras*. The court found that the arming and training of the *contras* for armed activities within Nicaragua also constituted a threat or use of force whereas "the mere supply of funds to the *contras*, while undoubtedly an act of intervention in the internal affairs of Nicaragua . . . does not in itself amount to a use of force." The court made no additional attempt to explain the bases for its demarcation. Some indirect intervention will be substantial enough to constitute prohibited force, and some will not.

In relation to the second question—what conduct constitutes an "armed attack" triggering resort to force in legitimate self-defense—the text of Article 51 offers no explanation and, again, the ICJ in the *Nicaragua* case provides helpful jurisprudence extracted here in some detail. The court determined:

> [t]here appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks. In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" *(inter alia)* an actual armed attack conducted by regular forces, "or its substantial involvement therein." This description, contained in Article 3, paragraph g, of the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law. The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it

---

50. *Id.* at 50, ¶ 227.
51. *Id.* ¶ 228.
52. *Id.*
been carried out by regular armed forces. But the Court does not believe that the concept of “armed attack” includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support. Such assistance may be regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States.53

The court relied upon the 1974 U.N. General Assembly Definition of Aggression and affirmed that the critical determining factor for satisfying the requisite threshold of an armed attack is “scale and effects” rather than the specific modalities of the deployment of force.54 It is unquestionably the case that cross-border deployment of regular armed forces constitutes an armed attack. If the cumulative scale and effects of cross-border raids (each of which individually may have constituted no more than a “mere frontier incident”) by irregular forces approximate those emanating from an armed attack by regular armed forces, according to the court, the self-defense exception applies.55 In 1986, this finding was a significant normative statement, and it has remained influential since. But the court was obviously keen to limit a potentially wide application of the norm. The final two sentences of the paragraph above reflect the court’s desire to pare back the scope of the norm. Sufficiently severe cumulative effects of cross-border raids may constitute an “armed attack,” but supply of weapons and logistical or other support will not be sufficient. That sort of support may constitute a threat or use of force, but it will not rise to the threshold of an “armed attack.”56

The court’s findings provide a response to the third question—what is the relationship between prohibited force and an “armed attack”—by identifying a normative gap between violations of the prohibition on resort to force and the right to respond with force to an armed attack. The court explicitly recognized this gap in declaring it “necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms.”57 The court had, after all, found that the supply of weapons to, and training of, the contras did constitute a use of force against Nicaragua, but that such interventions were not sufficiently grave to constitute an armed attack triggering the right to respond with force in self-defense. Michael Schmitt deftly articulates the approach of the court as clarifying the existence

53. Id. at 14, ¶ 195.
54. See id.
56. See id. at *543 (dissent).
57. Id. at ¶ 191.
of “a normative schema in which all armed attacks are uses of force, but not all uses of force are armed attacks.”

The court’s emphasis on consequential effects rather than on means or modalities for the deployment of force has been repeatedly reaffirmed. For example, in its 1996 Nuclear Weapons Advisory Opinion, the court declared the choice of weapon to be immaterial to the application of the normative framework on the use of force:

These provisions [Articles 2(4), 51 and 42 of the U.N. Charter] do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons. A weapon that is already unlawful per se, whether by treaty or custom, does not become lawful by reason of its being used for a legitimate purpose under the Charter.

In the aftermath of 9/11, the U.N. Security Council implicitly characterized the events of that fateful day as constituting an armed attack by explicitly recognizing “the inherent right of individual or collective self-defense in accordance with the Charter.” Intriguingly, the United States could only have used this recognized right of self-defense to defend itself against any future attacks and not against the attacks that already occurred. It is difficult to imagine how anyone could seriously argue that the 9/11 operations constituted anything less than an “armed attack,” given the scale of the loss of life and the physical destruction, let alone the devastating economic and security flow-on effects. The horrific incidents of 9/11 reaffirm the importance of focusing on scale and effects rather than on a narrow categorization of weapon types that fit the descriptor “armed.” As the events of that fateful day so spectacularly demonstrate, fueled civilian aircrafts can pose as formidably destructive “weapons.”

The Tallinn Manual applies a normative framework to cyber operations. Rule 11, the Definition of the Use of Force, and Rule 13, Self-Defence Against Armed Attack, unsurprisingly adopt a “scale and effects” approach to determine both threshold questions: (1) whether a cyber operation qualifies as a use of force; and, if so, (2) whether the operation reaches the “most grave” level of an “armed attack” triggering the right to respond with force in self-defense. For example, the Tallinn Manual asserts that “[a]cts that in-

60. Id.
61. See S.C. Res. 1368 (Sept. 12, 2001); see also S.C. Res. 1373 (Sept. 28, 2001).
jure or kill persons or damage or destroy objects are unambiguously uses of force." Analogous to the ICJ’s characterization of indirect U.S. intervention in Nicaragua through support to the contras, the international group of experts formed the view that “merely funding a hacktivist group conducting cyber operations as part of an insurgency would not be a use of force” whereas “providing an organized group with malware and the training necessary to use it to carry out cyber attacks against another State would . . . qualify.”

Beyond these specific examples, it is impossible for the Tallinn Manual to precisely determine the demarcations of both thresholds. The ICJ had the relatively easier task of applying the legal framework to the specific facts of the Nicaragua case, and the judges repeatedly asserted that they were restricted to answering the legal questions set forth by the parties. In contrast, the Tallinn Manual attempts to identify the generally applicable legal framework to cyber operations, and the best way the international group of experts could do this was through identifying illustrative examples of cyber operations. The Tallinn Manual acknowledges this limitation and identifies a number of qualitative indicia that states are likely to take into account in any use of force assessment. The identified indicia include severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality of any cyber operations. None of these indicia alone are intended to be determinative of the use of force. Instead, they are listed as likely qualitative indicators.

Nicholas Tsagourias is skeptical of the identification of qualitative indicia. He concedes that the Tallinn Manual acknowledges that the indicia are neither exhaustive nor legal, but he adds “whether they provide any guidance

63. Id. at 48 ¶ 8.
64. Id. at 46, ¶ 4.
66. See generally TALLINN MANUAL, supra note 20.
67. Id. at 48–51, ¶ 9.
68. Id.
69. Id. at 48, ¶ 9.
70. Id.
Despite Tsagourias’s skepticism, it is difficult to imagine what alternative course of action remained open to the international group of experts. One possibility would have been to argue that the Tallinn Manual must remain silent on operations that fall short of the threshold and the grave operations that rise to the level of “armed attack,” since there is such lack of clarity around the demarcations surrounding the use of force. However, given the rationale for the Tallinn Manual, such a position would constitute abject failure because the Tallinn Manual is intended to help provide clarification to states.73 Perhaps it is too early to say whether or not the indicia will be useful to states in deciding how to characterize particular operations against them and possible responsive measures. However, Tsagourias’s comments confirm that the mere publication of the indicia is generating a discussion that would not have occurred without the preparedness of the international group of experts to articulate their position.

Michael Schmitt identified the indicia he considered likely to “influence assessments by states as to whether operations amounted to a use of force”74 over a decade before the Tallinn Manual was drafted. In a subsequent article revisiting the jus ad bellum and cyber operations, Schmitt helpfully applied his indicia to the network attacks on Estonia in 2007.75 His analysis illustrates how the indicia might be applied by States:

Although [the attacks against Estonia] caused no deaths, injury, or physical damage, the attacks fundamentally affected the operation of the entire Estonian society. Government functions and services were severely disrupted, the economy was thrown into turmoil, and daily life for the Estonian people was negatively affected. The consequences far exceeded mere inconvenience or irritation. The effects were immediate and, in the case of confidence in government and economic activity, wide-spread and long-term. They were also direct, as with the inability to access funds and interference with the distribution of government benefits. Since some of the targeted systems were designed to be secure, the operations were highly invasive. While the consequences were severe, they were difficult to quantify, since most involved denial of service rather than destruction of data. Although political and economic actions are presumptively legitimate in use-of-force terms, these operations constituted more than merely pressuring the target state. Instead, they involved intentionally frustrating governmental

72. Id.
73. TALLINN MANUAL, supra note 20, at 3.
and economic functions. Taken together as a single “cyber-operation”, the incident arguably reached the use-of-force threshold. Had Russia been responsible for them under international law, it is likely that the international community would have (or should have) treated them as a use of force in violation of the [U.N.] Charter and customary international law.76

Schmitt readily concedes the imprecision of his indicia and the concomitant reality that states will have significant latitude in their characterization of cyber operations.77 Tsagourias is dubious about the merits of Schmitt’s (and the Tallinn Manual’s) indicia and illustrates his concerns by application of the indicia to the effects of the “Stuxnet worm.”78 Despite the damage to Iranian centrifuges and the setbacks the worm caused to the Iranian nuclear program, Tsagourias is unconvinced that the operation reached the threshold of a use of force on the basis of the application of the Tallinn Manual’s indicia.79 The quantification of damage and the precise de minimis threshold for a use of force are obvious challenges to the characterization of cyber operations. Schmitt is undoubtedly correct that clarification of these uncertainties in the application of the normative threshold will come as state practice develops in response to increasingly frequent and severe cyber operations.80 Perhaps until that state practice emerges, we are left with conjecture about precisely how states will apply the normative framework.

B. The Jus in Bello and Cyber Operations

The key reference to the term “attack” in the jus in bello appears in Article 49(1) of Additional Protocol I of 1977.81 That provision defines “attacks” for the purpose of the scope of application of LOAC as “acts of violence against the adversary, whether in offence or defence.”82 So defined, “attack” is a term of art. The ICRC’s Commentary on the Additional Protocols duly explains that, in the context of LOAC, “attack” should not be given the ordinary meaning of “striking the first blow,” but equated to “combat action” more broadly.83 However, the Commentary does not attempt to explain what “violence” means or, for that matter, what “combat action” entails.

76. Id.
77. Tsagourias, supra note 71, at 23–25.
78. Id.
79. Id. at 23.
80. Schmitt, supra note 75, at 578.
82. Id.
83. Id. at 603.
The threshold requirement for the application of LOAC is the existence of an armed conflict—not merely the existence of "attacks." Neither the Geneva Conventions nor the Additional Protocols define "armed conflict." Instead the treaty texts state the circumstances in which the treaties apply and, in the case of Additional Protocol II, also the circumstances in which that particular Protocol does not apply. The Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia (ICTY), in response to Dusko Tadić's interlocutory challenge to the Tribunal's jurisdiction, stated: "[A]n armed conflict exists whenever there is a resort to armed force between States or protracted violence between governmental authorities and organized armed groups or between such groups within a State." This definitional statement has become the standard formulation reaffirmed in all subsequent international criminal trial jurisprudence, including most recently at the International Criminal Court in all international trials involving war crimes charges. The definition reflects the treaty provisions on scope of application and distinguishes requisite thresholds for international and non-international armed conflicts. An international armed conflict requires a much lower threshold and exists "whenever there is a resort to armed force between [s]tates." A non-international armed conflict requires a much higher threshold of "protracted violence between governmental authorities and organized armed groups or between such groups within a [s]tate." This latter threshold has been clarified in repeated jurisprudence to require the satisfaction of a sufficient level of intensity in the exchange of hostilities and a sufficient level of organization of each of the non-state armed groups party to the conflict. Given the allegations against North Korea and China in relation to the Sony and OPM hacks respectively, this arti-

84. See id. at 39, 41, 46, 1343.
85. See id. at 1380.
88. For a more detailed analysis of the threshold requirements for the application of LOAC, see Caitlin Dwyer & Tim McCormack, Conflict Characterisation, in Routledge Handbook of the Law of Armed Conflict (Rain Liivõja & Tim McCormack eds.) (2016).
89. See Tadic, Case No. IT-94-1-I, at ¶ 70.
90. See id.
91. See, e.g., Al Bahlul, 820 F. Supp. 2d at 1181.
article will focus primarily upon the criteria for the existence of an international armed conflict.

It is an accurate normative statement that where two or more states oppose each other through cyber operations involving conduct constituting Article 49 application programming interface (API) attacks "conducted by, or attributable to, a [s]tate,"92 an international armed conflict exists, and the relevant LOAC applies. There are, however, a number of important threshold prerequisites to satisfy. First, attribution to a state is critical. Given that cyber operations are invariably designed to obfuscate the responsibility trail, this threshold preliminary issue will not necessarily be straightforward.93 Although a state need not be directly involved through its armed forces, the conduct of any of its agencies, including its intelligence or its law enforcement agencies, will also be attributable to the state.94

There is an additional threshold issue as to the requisite level of violence. The prevailing view is that no particular degree of violence or intention is required for the existence of an international armed conflict; it is sufficient that there be "a resort to armed force between [s]tates."95 The Tallinn Manual reaffirms this prevailing view but also identifies a competing view, which "requires greater extent, duration or intensity of hostilities although proponents of this view have not agreed on any particular threshold."96 The rationale for the competing view is that not all isolated incidents "such as sporadic border clashes or naval incidents" have been treated as international armed conflicts.97 The Tallinn Manual cites the Stuxnet operation as illustrative of the difficulties in determining requisite levels of armed force for the existence of an international armed conflict.98 The release of the Stuxnet malware caused significant physical damage to centrifuges in Iran’s nuclear fuel processing plant, but the international group of experts could not agree on whether the damage was sufficient to trigger an international armed conflict.99

Assuming, for the purposes of the analysis, that an international armed conflict does exist and that cyber operations are being conducted in the con-

94. See Schmitt, Classification of Cyber Conflict, supra note 92, at 252.
95. This view is consistent with the ICRC Commentary to Common Article 2 to the Four Geneva Conventions of 1949, for example.
96. TALLINN MANUAL, supra note 20, at 83.
97. Id.
98. Id.
99. Id. at 83–84.
text of that armed conflict, there remains an important question about what conduct will constitute an “attack” within the meaning of Article 49 of Additional Protocol I. As explained above, the ICRC Commentary to Article 49 does not attempt to explain what “violence” means or, for that matter, what “combat action” entails. The *Tallinn Manual* addresses this question in its Rule 30 Definition of Cyber Attack: “A cyber attack is a cyber operation, whether offensive or defensive, that is readily expected to cause injury or death to persons or damage or destruction to objects.”

The influence of the text of Article 49 of Additional Protocol I is apparent in the phrase “whether offensive or defensive,” but the Rule goes beyond the treaty text and the ICRC Commentary by focussing on expected violent effects. Here the approach is redolent of the emphasis on “scale and effects” in the *Tallinn Manual’s* articulation of relevant *jus ad bellum* Rules.

The *Tallinn Manual’s* Commentary refers explicitly to Article 49 of API and asserts that resorting to violence distinguishes attacks from other military operations. Consequently, non-violent operations, “such as psychological cyber operations or cyber espionage, do not qualify as attacks.” Popular misunderstandings aside, it is difficult to imagine any serious challenge to the normative veracity of this statement. Article 49 of Additional Protocol I does, however, refer to “acts of violence,” which could be interpreted narrowly to mean that the modality of the conduct must be violent rather than that the conduct generates violent consequences or effects. Here the Commentary to the *Tallinn Manual* demonstrates that the law of armed conflict has already moved on from such a narrow interpretation. Weapons of mass destruction—chemical, biological, and nuclear—do not rely on kinetic force for their destructive effects, and yet their deployment in armed conflict unquestionably constitutes an attack subject to the law of armed conflict. Additionally, the international group of experts observe that the text of many provisions of Additional Protocol I support this emphasis on effects. They cite as examples: (a) Article 51(1) protecting the civilian population and individual civilians from dangers arising from military operations; (b) the rule on proportionality in Articles 51(5)(b), 57(2)(a)(iii) and 57(2)(b) mandating the requisite calculus to include the expected “loss of civilian life, injury to civil-

100. *Id.* at 106.
101. *Id.*
102. *TALLINN MANUAL, supra* note 20, at 106.
103. *PILLOUD & DE PREUX, supra* note 81, at 605.
104. *TALLINN MANUAL, supra* note 20, at 106–07. Bill Boothby amplifies this argument. The willful release of deadly diseases, for example, does not involve kinetic force, but would anyone seriously argue that an act of violence involving biological warfare absent other acts involving kinetic force could not constitute an ‘attack’? See Bill Boothby, *Where Do Cyber Hostilities Fit in the International Law Maze?*, in *NEW TECHNOLOGIES AND THE LAW OF ARMED CONFLICT* 59, 60 (Hitoshi Nasu & Rob McLaughlin eds.) (2014).
ians, *damage* to civilian objects or a combination thereof”; (c) Article 55 on protection of the environment referring to “widespread, long-term and severe *damage*”; and (d) Article 56 protecting works and installations containing dangerous forces from attack where such attacks may *cause severe losses* among the civilian population.\(^{105}\)

Here, the issue is the scope of acts regulated by the law of armed conflict. The *Tallinn Manual* takes a broader approach by focussing upon the violent effects of conduct rather than on whether the conduct itself is violent.\(^{106}\) But the international group of experts “agreed that *de minimis* damage or destruction does not meet the threshold of harm required by this Rule.”\(^{107}\) Knut Dörmann of the ICRC takes an even broader approach.\(^{108}\) He argues that since the definition of a military object in Article 52(2) of Additional Protocol I refers to the neutralization of an object as a possible outcome of an attack, even the disabling of a legitimate military object (which may not constitute damage and certainly would not constitute destruction), also qualifies as an attack regulated by the law of armed conflict.\(^{109}\)

Rain Liivoja and Tim McCormack have commented elsewhere on the approach of the *Tallinn Manual* to the requisite level of damage or destruction for conduct to constitute an attack regulated by the law of armed conflict. One strength of the *Tallinn Manual* is the recurrent articulation of divergent views, in particular, the reference “to whether interference with the functionality of an object could amount to an attack in the absence of physical destruction.”\(^{110}\) The Commentary explains that a minority of experts believe that loss of functionality alone could never constitute an attack.\(^{111}\) However, the majority believe such an interference could qualify as “damage”; thus, the operation could constitute an attack “if restoration of functionality requires replacement of physical components”.\(^{112}\) The majority disagree, however, as to whether the damage requirement would be met if functional-

---

106. *Id.*
107. *Id.*
109. *Id.* at 142–43.
112. *Id.*
ity could be restored by reinstalling the operating system (i.e., "replacement" of the software).113

The Tallinn Manual’s general approach of insisting on physical detrimental effects from the destruction of data results in any such destruction qualifying as an attack only when it “results in the injury or death of individuals or damage or destruction of physical objects.”114 Our analysis of this conclusion was that it:

is not entirely unproblematic. Permanent destruction of data can have significant ramifications, even though falling short of physical violence. For example, wiping out the data in the entire State’s banking system or patent database by means of a computer virus may have far more deleterious consequences than the physical destruction of a single data centre. Yet, under the Manual, the former would be an attack only if it can be demonstrated that some physical injury occurred, whereas the second is undoubtedly an attack. This peculiarity is remedied slightly by the admission that causing ‘serious illness and severe mental suffering that are tantamount to injury’ would qualify as an attack. Thus terrorising the civilian population by means of cyber operations might rise to the level of attack. Accordingly, were the cyber operations against the banking system serious enough to cause wide-spread panic among the population, the argument could be made that the mental suffering of the civilians was such as to qualify the operation as an attack.

The Manual arguably fails to take the destruction of data and the value of digital assets sufficiently seriously. To a large extent this reflects the current conceptual framework of LOAC, which has not entirely caught up with the development of the concepts of intellectual property and intangible assets. But the Manual’s general position on the destruction of data seems curious in view of the fact that in Rule 82 it regards the destruction of digital cultural property perfectly governable by LOAC. Certainly, the use of the term ‘property’ in the context of cultural treasures may more readily allow for the incorporation of intangible assets, but the time has perhaps come to seriously consider whether an ‘object’ for the purposes of the targeting rules in LOAC necessarily needs to have corporeal existence.115

Identifying the relevant legal framework regulating cyber operations is a relatively straightforward exercise. As the Tallinn Manual’s Commentary and scholarly critiques of the Tallinn Manual and its commentary demonstrate, the substantially more complex issue is the application of that legal

113. Id.
114. Id.
framework to contemporary, and no doubt future, cyber operations. Future state practice will reveal the extent to which existing analysis is useful and will undoubtedly be closely scrutinized to determine how states interpret and apply the law. Any relevant jurisprudence from courts and tribunals involving the interpretation and application of the normative framework to specific facts will also be helpful in the clarification of the law. But it would be fallacious to assume that existing uncertainties will evaporate in the face of states’ responses to cyber operations against them.

III. CHARACTERIZING THE OPM AND SONY “ATTACKS”

Attribution is a critical preliminary issue for the international legal characterization of the OPM and Sony “attacks” and for any determination of responsive measures the United States could lawfully undertake. Stealth and the obfuscation of responsibility are often integral to cyber operations. Yet the application of the normative framework is dependent upon attribution of international legal responsibility to states.

On December 19, 2014, just weeks after the Sony “attack,” the Federal Bureau of Investigation (FBI) announced that it had sufficient evidence to conclude that the North Korean government was responsible. Although unwilling to disclose all its evidence, the Bureau’s press release cited commonalities with data-deletion malware, IP addresses, and modalities of a cyber operation against South Korean banks and media outlets—all previously utilized or undertaken by North Korea. There is skepticism in some circles about the veracity of the FBI’s determination, but it is unusual for the U.S. authorities to name those responsible so unequivocally and so relatively soon after a damaging cyber hack. The United States was much more equivocal, for example, about attribution of responsibility for the OPM hack. Although many suspected Chinese responsibility for the theft of sensitive OPM data, senior U.S. officials quickly denied any certainty about attribution of respon-


117. Id.


sibility.120 More recently, media reports suggest that China arrested several individuals for the OPM attack and has attempted to distance the state from any responsibility.121 Unidentified U.S. officials were reported to say that “it has been difficult to confirm whether the people rounded up were connected to the OPM breach,” but that “[i]f China caught the real perpetrators, ‘it would be the most important arrest that we’ve perhaps seen in cybercrime.”122

For the purposes of the present discussion, let us assume, hypothetically, that international legal responsibility could be attributed to North Korea and China for the Sony and OPM hacks, respectively. In reality, of course, such attribution is far from certain, but the hypothetical assumption facilitates the subsequent legal characterization.

Turning first to the jus in bello, it is difficult to argue that either the Sony or the OPM hacks triggered an international armed conflict between the United States and North Korea or China, respectively. Despite popular calls to recognize these hacks as “acts of war,” it is reassuring that the Obama administration has steadfastly refused to characterize either hack as such.123 Despite the prevailing view that an international armed conflict exists whenever there is “a resort to armed force between States” and that no particular threshold of violence or intention is required,124 the counterview that not all isolated incidents “such as sporadic border clashes or naval incidents” have been treated by states as international armed conflicts125 is reassuring. Imagine the possibilities for escalation and devastation if the United States considered the Sony and OPM hacks as tantamount to declarations of war and responded accordingly.

Another jus in bello consideration arises if we assume, hypothetically, that the Sony and OPM hacks each occurred in the context of existing international armed conflicts between the United States and North Korea, and between the United States and China, respectively. In such circumstances, would either hack amount to an attack within the meaning of Article 49 of


122. Id.

123. Sheppard, supra note 13.

124. TALLINN MANUAL, supra note 20, at 82–83, ¶ 12.

125. Id.
Applying the approach of the *Tallinn Manual*, the OPM hack would not seem to satisfy the criteria. No loss of life or injury to persons ensued, and no physical damage or destruction was caused. Such analysis might change depending upon how, if at all, the data is used. If identity fraud, for example, becomes rampant against many of those whose personal information was stolen, injury and damage may well become a reality. Meanwhile, however, the U.S. government reportedly characterizes the hack as cyber espionage—"spying to help a foreign government, in this case, build databases on U.S. government employees and officials." The analysis here is different for the Sony hack. Although, again, no death or physical injury to persons occurred, there was some damage in that Sony lost the functionality of thousands of its personal computers. While it could be argued that the malware did not physically damage or destroy the individual units of hardware, they were rendered useless. On loss of functionality, the majority of the *Tallinn Manual* experts considered that "if restoration of functionality requires replacement of physical components," such loss constitutes damage and qualifies as an attack. A few experts went so far as to suggest "interference with functionality that necessitates data restoration, while not requiring physical replacement of components or reinstallation of the operating system, qualifies as an attack." Even if the damage to Sony were sufficiently serious to qualify as an attack, given that there was no international armed conflict between the United States and North Korea, such analysis is of limited practical consequence.

Perhaps the more significant legal analysis involves the application of the *jus ad bellum*. Neither the Sony nor the OPM hacks are sufficiently grave to constitute armed attacks justifying a forceful response by the United States in self-defense, and it is perhaps unsurprising that the United States has chosen not to characterize them as such. Neither hack resulted in loss of life or physical injury. Both hacks involved the exfiltration of massive amounts of sensitive data and, in the case of Sony, the loss of functionality of thousands

128. See id.
129. Nakashima, supra note 212.
131. See id.
133. Id. at 109, ¶ 11.
134. See Sheppard, supra note 13.
of personal computers.\textsuperscript{135} Even this latter physical damage could hardly be characterized, “because of its scale and effects,”\textsuperscript{136} as amounting to an armed attack. Perhaps if each of the Sony buildings, in which personal computers were housed, had been destroyed, the cumulative effect of any such strikes may well have risen to the level of an armed attack. But that is not what happened. Sony’s buildings and other infrastructure remain intact and the corporation continues to operate.\textsuperscript{137}

However, it is arguable that the damage to the functionality of Sony’s personal computers constituted a use of force short of an “armed attack.” The Tallinn Manual’s assertion that “[a]cts that injure or kill persons or damage or destroy objects are unambiguously uses of force”\textsuperscript{138} arguably applies here. The counter argument is, as above, that the malware only targeted the functionality of Sony’s computers and did not physically damage or destroy the individual units of hardware.\textsuperscript{139} But if Sony was required to replace all the individual units, the gravity of the hack would be more pronounced and the United States would be more likely to consider the hack an unlawful use of force. Even if the level of damage did not rise to the requisite threshold, the United States would nevertheless be entitled to reach the same conclusion as the ICJ in its characterization of the United States’ financing of the contra rebels: the Sony hack constituted a violation of the U.S. sovereignty through an unlawful intervention in its internal affairs.\textsuperscript{140}

\begin{itemize}
  \item \textsuperscript{135} See Hess, supra note 130.
  \item \textsuperscript{136} Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶195 (June 27).
  \item \textsuperscript{138} Tallinn Manual, supra note 20, at 48, ¶8.
  \item \textsuperscript{139} See Hess, supra note 130.
  \item \textsuperscript{140} See G.A. Res. 36/103, U.N. Doc. A/RES 36/103 (Dec. 9, 1981). In 1981, for example, the U.N. General Assembly adopted the Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, and, inter alia, affirmed the following:

  The right of States and peoples to have free access to information and to develop fully, without interference, their system of information and mass media and to use their information media in order to promote their political, social, economic and cultural interests and aspirations, based, inter alia, on the relevant articles of the Universal Declaration of Human Rights and the principles of the new international information order.

  Id. At stake in the hack on Sony was the U.S. Constitutional right of Freedom of Expression and specifically the freedom of the Sony Corporation to publicly release the movie The Interview—a parody of the North Korean leader Kim Jong Un. Id.
Unlawful intervention raises the possibility of countermeasures: conduct recognized by international law as a permissible response to intervention intended specifically to convince another state to cease and desist from its illegal conduct.\textsuperscript{141} Article 22 of The International Law Commission’s \textit{Draft Articles on Responsibility of States for Internationally Wrongful Acts} affirms the permissibility of conduct that would otherwise constitute a violation of international law in certain limited circumstances, and the ICJ has reaffirmed the doctrine of countermeasures and identified the criteria that must be satisfied.\textsuperscript{142} The \textit{Tallinn Manual} discusses countermeasures to cyber violations of a State’s sovereignty that do not amount to an “armed attack,”\textsuperscript{143} and Michael Schmitt explains, in his own detailed analysis of the subject, that countermeasures to unlawful cyber operations are all too frequently overlooked.\textsuperscript{144} Only States can lawfully undertake countermeasures and only in response to unlawful intervention attributable to other States.\textsuperscript{145} The Sony Corporation could not, therefore, lawfully undertake countermeasures itself but, presumably, the United States could do so on its behalf, assuming all other prerequisites (the nature of the hack and the damage it caused, the hack was attributable to North Korea, and any countermeasure is proportionate to the injury suffered) are satisfied.\textsuperscript{146}

For hacks like that of the OPM, which constitute cyber espionage and are not unlawful, the prospect of U.S.-China collaboration on accountability for those responsible is intriguing. Although it is still too early to tell whether the individuals arrested by Chinese authorities are indeed responsible for the OPM hack, if that proves to be the case and those individuals are successfully prosecuted in Chinese courts, the experience will be a landmark in U.S.-Chinese co-operation on the investigation of malicious cyber operations. It would be ironic if the emergence of a mutual interest in the prevention of damaging reciprocal cyber espionage provided a catalyst for improved Sino-U.S. relations.


\textsuperscript{143} See \textit{Tallinn Manual}, supra note 20, at 36–41.


\textsuperscript{145} See id. at 703, 707.

\textsuperscript{146} See id. at 723.