INTERNATIONAL LAW STUDIES

PUBLISHED SINCE 1895

U.S. NAVAL WAR COLLEGE

The Cyber Road Ahead: Merging Lanes and Legal Challenges

Kenneth Watkin

89 INT'L L. STUD. 472 (2013)

Volume 89 2013

The Cyber Road Ahead: Merging Lanes and Legal Challenges

Kenneth Watkin[*]

I. INTRODUCTION

It is a bit daunting to think about the "road ahead" when the concept of cyber warfare is just entering the public discourse. Fueled first by cyber "attacks" in Estonia and then in Georgia,[1] the dialogue has gotten louder with revelations about a cyber conflict occurring as part of the "covert" campaign to disrupt the nuclear program of Iran.[2] Terms such as "Stuxnet," "Duqu" and "Flame" have now entered the public cyber lexicon.[3] How international law should regulate the use of this technologically advanced domain with regard to the recourse to war (the *jus ad bellum*), and as method

* Brigadier-General, Canadian Forces (Ret.); Former Judge Advocate General for the Canadian Forces; 2011–12 Charles H. Stockton Professor of International Law at the U.S. Naval War College.

1. For an outline of cyber warfare in the twentieth and twenty-first centuries involving Israel, Chechnya, Estonia, Georgia, North Korea, Iran and the United States, see JEFFREY CARR, CYBER WARFARE 2–3 (2009).

2. Gary D. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, 63 JOINT FORCE QUARTERLY 70 (2011), *available at* http://www.ndu.edu/press/why-iran-didnt-admit-stuxnet.html.

3. Nicole Perlroth, *Researchers Find Clues in Malware*, NEW YORK TIMES, May 31, 2012, at B1, *available at* http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stux net-and-duqu.html.

and means of warfare (the *jus in bello*) has become the subject of substantial legal scrutiny.[4]

The contemporary discussion of cyber threats speaks not only of danger, but often also of catastrophe. In this regard it is not uncommon to hear of cyber "Pearl Harbors"[5] and for cyber "weapons" to be equated to implements of mass destruction based on what has been termed a "microforce," similar to chemical and biological armaments.[6] In addition, it has been suggested that "[t]he conventions and applicable case law on nuclear warfare are relevant to controlling the scope and tools of [information warfare]."[7] The use of the term "information warfare" reflects an almost schizophrenic discussion that includes soft concepts like preserving or exploiting information, and bellicose words, such as attacks.[8]

As a microforce, cyber presents a significant communication challenge for anyone attempting to explain how it works and why anyone should be worried about its capabilities. It is difficult to suggest that cyber is a threat of exceptional proportions when cyber means are trending in the opposite direction with ever shrinking hardware. Explanations of the cyber domain often result in a dialogue wrapped in a mysterious language of "clouds," "viruses" and "botnets." Reflecting its nascent status in terms of regulation, the language of cyber incorporates a breathtaking range of seemingly un-

---

4. *See* TALLINN MANUAL ON THE LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013); CYBER WARFARE: CRITICAL PERSPECTIVES (Paul Ducheine et. al. eds., 2012).

5. Jason Ryan, *CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor*, ABC NEWS (Feb. 11, 2011), http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905#.UHLoS7SqCME.

6. In assessing "digital warfare," one the author notes:

> Compared to other types of military force, digital warfare represents a type of microforce. The distinction is analogous to the difference drawn between conventional military forces employing chemical explosives or kinetic energy as their primary means of achieving effect versus the megaforce unleashed by nuclear weapons based on the fission or fusion of atoms. At issue here is the amount of energy unleashed by a given weapon at the time of attack. Weapons across the micro-conventional-mega force spectrum can all cause very significant impacts. Chemical or biological weapons are referred to as weapons of mass destruction, not because of the amount of destructive energy released when they are deployed but because of the number of deaths they can cause. . . . Despite the microforce nature of information attacks, disruption of the digital control systems of a nuclear power plant could cause similarly large-scale effects.

GREGORY RATTRAY, STRATEGIC WARFARE IN CYBERSPACE 20 (2001)

7. *See also* Scott J. Shackleford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKLEY JOURNAL OF INTERNATIONAL LAW 191, 217 (2009).

8. *Id.* at 198–99.

connected concepts that appear more closely aligned to advertising, science fiction and biological threats, although it can also take on a more bellicose connotation in its reference to attacks. This language can be problematic for those seeking to come to grips with the domain and, importantly, communicate its dangers within governments and to the broader public.

At times, there can be an overriding sense that the public is only now learning what States are being forced to reveal.[9] Cyber is a creature of technological advancement. As often occurs, the technology has developed well ahead of the limiting framework States use to keep its advances in check. In this regard, the road ahead appears to be one with two merging lanes. One path is a technological, with advances occurring at apparently prodigious speed. Such developments are limited, it would seem, only by the imagination of their creators. The other lane is one where the policy, ethical and ultimately legal constraints of society are being test driven even as they are being developed. In a sense this is a phenomenon that has been seen before as society struggled to control the development of chemical and nuclear weapons and air warfare following World Wars I and II.

However, there is a fundamental difference in the twenty-first century. At no point were the twentieth century weapons readily available to the world's population. It was estimated in 2008 there were one billion personal computer users worldwide, a figure expected to double by 2014.[10] Among those users are teenagers keen on social networking or testing their ability to challenge the rules imposed on them by society. It is a world that also includes hacktivists, like the group Anonymous, whose penetration of government, business and organizational websites raises security concerns, but is not readily associated with legal concepts such as armed attack and armed conflict.[11]

---

9. Scott Shane, *Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials*, NEW YORK TIMES, Sept. 27, 2012, at A10, *available at* http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html?pagewanted=all ("Just as drone-fired missiles have never been a secret to those on the ground, so cyberattacks have consequences that cannot be hidden, even if their origin may be initially uncertain.").

10. *Computers in use pass 1 billion mark: Gartner*, REUTERS (June 23, 2008), http://www.reuters.com/article/2008/06/23/us-computers-statistics-idUSL2324525420 080623.

11. Devlin Barret, *Retaliation Fears Spur Anonymity in Internet Case*, WALL STREET JOURNAL, Jan. 28, 2012, at A3, *available at* http://online.wsj.com/article/SB10001424052970203363504577185364 230417098.html ("Anonymous is a loose affiliation of hackers and activists who are self-proclaimed protectors of Internet freedom. To the Justice Department, the group is something more sinister. More than a dozen alleged members have

The "information superhighway" that forms the backbone of the cyber domain is truly a crowded thoroughfare.[12] What is not known at this stage is whether the intersection of the two lanes along this cyber road stretching into the future will be the scene of a tremendous clash of cultures (one technological and the other societal) or a seamless integration that restricts cyber as a means of warfare to help meet the security needs of States, while being constrained by humanitarian demands in its application.

One can be skeptical regarding the accuracy of the forecasts of cyber Armageddon with the advent of cyber warfare. Although it has largely now disappeared from the contemporary cyber dialogue, in 1999 there were predictions by the technical community of a potential "catastrophe." However, this one was in the nature of a self-inflicted wound. Apparently, in the early days of computer development:

> [P]rogrammers sought to economise on then-scarce computer storage space by writing dates with two digits for the year instead of four. These programmers either failed to consider the implications of the end of the 20th century or assumed that their systems would have been scrapped long before then. By the time the problem was taken seriously in the mid-1990s, code with two-digit dates was said to be ubiquitous, occurring not only in conventional computer systems but in 'embedded systems' such as those in automatic lifts, air navigation systems and so on. While the exact consequences of these problems were beyond anyone's imagination, widespread system failures could be anticipated on 1 January 2000, and the cascading effect of these failures was expected to cause, at a minimum, severe economic dislocation.[13]

The Y2K concern is of particular relevance to twenty-first century discussions about cyber warfare. It involved the resilience of the machines and systems, such as the supervisory control and data acquisition (SCADA)

---

been charged with computer crimes; they have pleaded not guilty. Anonymous has no formal structure or membership, and in some ways is more of a banner under which hackers and others choose to operate than an actual organization.").

12. "Information superhighway" is defined as "an extensive electronic network such as the Internet, used for the rapid transfer of information such as sound, video, and graphics in digital form." OXFORD DICTIONARIES ONLINE, http://www.oxforddictionaries.com (last visited Oct. 3, 2012).

13. John Quiggan, *Y2K Scare: Causes, Costs and Cures*, 64 AUSTRALIAN JOURNAL OF PUBLIC ADMINISTRATION 46 (2005), *available at* http://www.uq.edu.au/economics/johnquiggin/JournalArticles05/QuigginAJPA05Y2K.pdf.

networks controlling electrical grids and pipelines,[14] and the impact of a critical failure of these machines that govern everyday life and harness the dangerous forces upon which modern civilized society is based.[15]

The result was a mobilization of large parts of the developed world to prepare for the turn of the century. In November 1999, it was estimated expenditures "by U.S. firms, non-profits and government agencies, in the years 1995 through 2001, will be in the neighborhood of $100 billion, or about $365 per U.S. resident."[16] Apparently the response was not uniform, as Europe and other parts of the world either reacted unenthusiastically or not at all.[17] In contrast, English-speaking countries paid particular attention to the perceived threat, not only because of their common language and historical ties, but also, it is suggested, as a result of reliance to various degrees on tort litigation as a means of social regulation.[18]

The rest is history, as uneventful as it was. The predictions proved very wrong. Perhaps the best summary is that provided by John Quiggan, who noted with regard to the Y2K "disaster" that "[f]rom the perspective of public administration, the two most compelling observations relate to conformity and collective amnesia."[19] Once a conformist response has been initiated, "no policy actors have any incentive to oppose, or even to critically assess, the dominant view."[20] Developed countries had become dependent upon new technology that apparently was not fully understood. This

---

14. For an outline of the threat that computer malware and hackers could have on SCADA systems, see RICHARD A. CLARKE & ROBERT K. KNAKE, CYBERWAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 98–101 (2010).

15. ECONOMICS AND STATISTICS ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE, THE ECONOMICS OF Y2K AND THE IMPACT ON THE UNITED STATES 7 (1999), *available at* http://www.esa.doc.gov/sites/default/files/reports/documents/y2k_1.pdf [hereinafter *United States Y2K Report*] (describing that "critical infrastructure . . . suggests facilities whose damage due to Y2K failures would cause a wide circle of disruptions. Damages may still essentially be local, however. In an economy as large as the United States, hundreds and perhaps thousands of failures in 'critical infrastructure' electricity or water systems could occur before the impact would be great enough before there would be a significant impact.").

16. *Id.* at 11.

17. Quiggan, *supra* note 13, at 49 ("The response to Y2K problems in non-English speaking countries was slower and less enthusiastic. . . . In Eastern Europe and less developed countries, the Y2K problem was almost entirely ignored in view of the more pressing concerns facing these countries.").

18. *Id.* at 53.

19. *Id.* at 54.

20. *Id.*

led to a perceived crisis. The Y2K incident suggests, perhaps, that with regard to claims regarding the impact of cyber warfare it would be prudent for legal advisors to have a degree of skepticism in assessing predictions of disaster.

Much has changed, however, since Y2K. Cyber is even more integrated into society. As a security issue, it is here to stay and appears to be capable of more than simple interference with our lives. Indeed, in addition to being integrated into our everyday life, cyber is also part of the national order of battle for over thirty countries.[21] It is assessed that at least twelve of the world's fifteen largest militaries are building cyber warfare programs."[22] For the United States, this means cyberspace is an operating domain on par with land, sea, air and space,[23] as well as one requiring dedicated command and units.[24] It is likely that the involvement of other countries in the military cyber realm will be considerably more modest. What is unclear is the degree to which cyber "have" countries will be, rightly or wrongly, more concerned with cyber threats and the dangers they pose because of risks to military capabilities or broader economic interests.[25]

Like Y2K, there is a danger that overemphasis on predictions of catastrophe will heavily influence how the threat is perceived and responded to by a State. The perception of the threat may also be affected by the tools available to the State to respond. This could mean that in countries without the same level of dedicated military resources as some developed countries the cyber challenge could be viewed as less military in nature. It may more naturally lead to discussion of alternatives to the use of force and increased international dialogue and cooperation. Of course, the challenge facing policy makers is whether those options are sufficient to confront the threat.

At the same time other States, which have not—or cannot—develop sophisticated cyber capabilities, may also have a particular interest in ensuring international law operates as a brake on the cyber warfare activities of the "have" States. There is nothing new in using the law for that purpose. It has been at the heart of the post-World War I and -World War II em-

---

21. INTERNATIONAL INSTITUTE FOR SECURITY STUDIES, THE MILITARY BALANCE 2011, at 27, 28–32 (2011) (assessing the military dimension of cyberspace).

22. Shane, *supra* note 9.

23. U.S. DEPARTMENT OF DEFENSE, QUADRENNIAL DEFENSE REVIEW REPORT 37 (2010).

24. *Id.* at 38–39.

25. *Id.* at 37 ("In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace.").

phasis on the *jus ad bellum* restrains on the recourse to war.[26] Therefore, while countries like the United States may seize the opportunity to shape the international legal discussion regarding regulation of the cyber domain, so will those countries that seek to reinforce the need for restraint.[27] In this respect, international law will need to reflect standards that apply to all countries.

In any event, all military cyber forces and their legal advisors will be faced with a number of challenges as the march down the cyber highway proceeds. The challenges can be placed into two broad categories: first, the prevalent, indeed predominate non-military use of cyber in society. Second, in a dialogue that is just starting to take place in a public way, is the need to reach consensus on how the international law can and should bring a potential technical "beast," made of "1s" and "0s," to heel on this very human journey down the cyber roadway. If the predictions of catastrophe are true, this makes the need for regulation all the more pressing. However, as will become evident, efforts to provide law and order in the cyber world will be challenged by the fact that as a policy option the use of cyber to influence the security environment seems so attractive.

This article will address these challenges in three parts. First, there will be an outline of a unique aspect of the cyber domain in the context of its status as a new global commons and its prevalence within modern society. As a result there will be many stakeholders who have views that will impact on the regulation of cyber activity. Second, the analysis will turn to specific legal challenges. This part will look at civilian participation in cyber conflict, consider the theoretical approaches applied when assessing cyber operations as a use of force, look at the use of the cyber domain for countermeasures short of war and address the significant potential for confusion at a foundational level regarding the use of the term "attack." Finally, the potential for successfully integrating cyber operations into a legal framework will be considered by reference to efforts during the twenty-first century to regulate technologically advanced aerial warfare. Ultimately the road ahead

26. Quincy Wright, *The Outlawry of War and the Law of War*, 47 AMERICAN JOURNAL OF INTERNATIONAL LAW 365, 368 (1953).

27. Shane, *supra* note 9 (Where Matthew Waxman is said to have noted that, whereas previous United States administrations had ceded ground to critics by remaining silent on drones and therefore allowing them to be portrayed as lawless, the U.S. government is now being more public with regard to cyber issues. As the United States "occupies a position of advantage on offensive cyber capabilities, it should seize the opportunity to lay out a set of rules for itself and others.").

will be identified as a challenging one, but with an attainable goal that will require flexibility in applying traditional legal principles to the cyber domain.

II. A VOICE AT THE TABLE?

A key challenge for those seeking to attract the attention of lawyers and policy makers regarding the dangers and opportunities of military cyber capabilities is getting a voice at the table that is heard and understood. To get a sense of the scope and scale of the challenge, it is useful to look at national policies regarding cyber. Consistent with the United States having an advanced cyber capability and the openness inherent in it being a democracy, that country has a number of publically available defense related documents on the issue.[28] It is the overarching 2011 national strategy document *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* that broadly defines the nature of the international cyber challenge.[29] It states:

> [D]igital infrastructure is increasingly the backbone of prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies. As never before, information technology is fostering transnational dialogue and facilitating the global flow of goods and services. These social and trade links have become indispensable to our daily lives. . . . The reach of networked technology is pervasive and global. For all nations, the underlying digital infrastructure is or will soon become a national asset.[30]

Of course, States must defend their national assets; however, this statement raises a number of profound issues. Can a State physically defend all of its national digital assets? What is the cost in terms of global discourse and, in particular, international commerce? If national assets are defended will it mean reduced, or even truncated, access to the computer sys-

---

28. *See, e.g.,* QUADRENNIAL DEFENSE REVIEW REPORT, *supra* note 23; U.S. DEPARTMENT OF DEFENSE, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf.

29. THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter *International Strategy for Cyberspace*].

30. *Id.* at 3.

tems that underpin the information superhighway for global participants? There is also the more mundane bureaucratic question of who needs to be sitting around the table at the highest levels of government to make those decisions in order to ensure the military imperatives are properly weighed against the economic and social costs of seeking to regulate the cyber domain.

Another fundamental issue is whether national assets effectively lose their parochial status because they are part of an interconnected network that "is pervasive and global."[31] Is the legal control of the digital world "territorial" in the sense of coming exclusively under State sovereignty? To a certain extent the answer to this question is yes. The international legal framework is founded on the concept of the post-Westphalian State. It simply makes sense that the regulation of a fundamentally international technology would be State-based and State-focused as well. This is not to take away from the role that international institutions play or the impact of increasing globalization, however, States "retain their attraction as the primary focus for the social activity of humankind and thus for international law."[32]

But the boundaries of national jurisdiction in the cyber world are not clear. The cyber environment can be equated to a global commons, such as the oceans, although it has also been noted that "unlike the other domains, cyberspace has no physical obstacles, nor 'real' boundaries like a shore."[33] The cyber domain is also unique in that it is manmade.[34] International regulation of the maritime domain has been slow but steady, as it has had to balance the rights of States, territorial jurisdiction, freedom of navigation and private economic interests. It has been noted that "[t]he story of the evolution of [the UN Convention on the Law of the Sea] is the imperative that the private sector must be given a place if real progress in regulating the commons is to be made."[35] Ultimately, the regulation of global commons, as is evidenced by the law of the sea, "ha[s] a significant effect on the exercise of both belligerent and neutral rights during time of armed

31. *See International Strategy for Cyberspace, supra* note 29, at 3.

32. MALCOLM N. SHAW, INTERNATIONAL LAW 197 (6th ed. 2008).

33. Frans Osinga*, Introducing Cyber Warfare,* in CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 5, at 9.

34. QUADRENNIAL DEFENSE REVIEW, supra note 23, at 37.

35. Shackelford, *supra* note 7, at 226.

conflict."[36] Private, particularly commercial, interests in the cyber domain will also have to be taken into account in the regulation of cyber conflict in much that same way that neutrality has impacted on international humanitarian law.[37]

Further, not all States have embraced international regulation of the oceans. While a State, like the United States, may have a significant interest in adopting the United Nations Convention on the Law of the Sea (UNCLOS), conflicting ideas of national security interests have prevented it from doing so.[38] The United States military supports ratification.[39] Rather than be bound by such regulation, however, a certain advantage has been perceived within the legislative branch of the United States government in the constructive ambiguity of having an international regime in place, but not being technically subject to its constraints.[40] The same result could occur regarding a number of the players in the cyber domain. Ambiguity often equates to freedom of action. Freedom, however, can come at the expense of other States understanding the motives and the potential action to be taken by a nation. It can also impact adversely on the issue of accountability.

It is also not clear how—or if—States and their military forces will want to embrace international regulation when the use of cyber for military

---

36. SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA 93 (Louise Doswald-Beck ed., 1995)

37. LESLIE GREEN, THE CONTEMPORARY LAW OF ARMED CONFLICT 297 (3d ed. 2008) ("Even in major conflicts involving a number of countries, including the most powerful, there are always some which remain outside the conflict and seek to assert their right as neutrals not to be interfered with by the belligerents.").

38. Thomas Wright, *Outlaw of the Sea*, FOREIGN AFFAIRS (Aug. 7, 2012), *available at* http://www.foreignaffairs.com/articles/137815/thomas-wright/outlaw-of-the-sea (Describing that the two objections in the United States Senate regarding ratification of UNCLOS are concerns over encroachment of the International Seabed Authority on United States sovereignty and "the treaty would prevent the U.S. Navy from undertaking unilateral action, such as collecting intelligence in the Asia-Pacific region, because permission to do so is not explicitly granted in the text").

39. *Id.* ("According to Admiral Samuel Locklear, commander of U.S. Pacific Command, however, the convention in no way restricts our ability or legal right to conduct military activities in the maritime domain. On the contrary, as U.S. Defense Secretary Leon Panetta puts it, U.S. accession to the convention 'secures our freedom of navigation and overflight rights as bedrock treaty law.'").

40. *Id.* ("[C]ritics point out, the ultimate indispensability of U.S. naval power means that the country can receive the benefits of the convention without being bound by it. Since the world seems to have functioned perfectly well in this halfway house for some time, it would make no sense to codify the convention now.").

operations has yet to be fully developed or exercised. Such reluctance may also impact the decisions of less dominant States that want to avoid controls on its use favored by a more dominant cyber power. A military cyber capability provides a potential asymmetric advantage that may be simply too attractive an option for those States seeking to level the security playing field.[41] As John Arquilla has noted, "[n]o country may be foolish enough to engage the incomparable U.S. military in open battle, but we seem like fairly easy pickings to the computer mice that may soon roar."[42] Rather, the pressure for regulation may ultimately come from major industrialized States once they feel threatened, since "dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by non-state actors."[43]

Given the pervasive role played by the cyber domain in modern society, it also is unlikely that national security law and policy makers will unilaterally determine the outcome of the cyber debate. The interests of individual States and the views of their military forces on what is needed for defense will be just two of the many voices at the table to discuss what, if any, rules are established to regulate the defense of the national cyber systems.[44] One issue will be the relative importance States place on potential threats in a defense context in relation to very real non-military cyber threats that States presently face. For countries, such as the United Kingdom and Canada, the relatively low prioritization of the cyber challenge in terms of defense is reflected in the limited space their national cyber strategies devote to the topic. Further, in reading national policies' references to "defense," the term cannot be assumed to have a military context as it often means protection against criminal activity and espionage. Substantive reference to

41. Richard Stiennon, *Is An International Cyber Regulatory Agency Needed?*, FORBES (Aug. 22, 2012), *available at* http://www.forbes.com/sites/richard stiennon/2012/08/22/is-an-international-cyber-regulatory-agency-needed/ ("I can imagine that the concept of such a treaty and regulatory body will not gain much traction in the military academies and think tanks around the world. Why restrict a nation's options in war fighting—especially when cyber weapons are inexpensive (compared to fighter jets, tanks, and aircraft carriers) and could reduce the overall level of force required to achieve an end goal?").

42. John Arquilla, *Cool War*, FP NATIONAL SECURITY (June 15, 2012), http://www.foreignpolicy.com/articles/2012/06/15/cool_war.

43. Osinga, *supra* note 33, at 10.

44. For an outline of the divergent views and priorities of bureaucratic actors when considering policy priorities "amid a rapidly evolving strategic environment," see Mathew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 436 (2011).

cyber and the role of military forces is usually found somewhere towards the back of the strategy.[45]

Although there appears to be much to defend in terms of its priorities, the subject of defense competes for space with privacy, business security products, cyber crime, cyber fraud and even the denial of safe havens to cyber criminals.[46] It appears that consideration of cyber "national defense," using the term in a *jus ad bellum* context, and the law that frames it in the post-UN Charter world, have been introduced rather late into the journey down the cyber roadway. This raises questions as to whether States have actually viewed the military threat to be as a grave as some would suggest, or whether it is criminal activity that is seen to form the most significant challenge.

The focus on issues other than cyber warfare is a reality and, in many respects, so it should be. Most citizens are more concerned with losing money from their bank account or a lowering of their credit rating than being the subject of an actual armed cyber attack that would cause the Security Council to meet to discuss two States having gone to war.[47] Cyber is different. More citizens rely on, and can relate to, the cyber realm. It is the predominance of cyber in the everyday lives of developed and, increasingly, less-developed States that will put considerable pressure on lawyers to closely consider how traditional security related concepts and principles of international law apply to this new form of warfare.

III. THE LEGAL CHALLENGE

A. Participation in Cyber Conflict

When thinking about the cyber domain, lawyers who work with national defense issues, in particular the use of military force may be challenged to rethink long-held notions of international law. For example, one area that

45. *See, e.g.,* CABINET OFFICE, THE UK CYBER SECURITY STRATEGY PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD ¶ 4.9 (2011), *available at* http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf [hereinafter *UK Cyber Security Strategy*]; GOVERNMENT OF CANADA, CANADA'S CYBER SECURITY STRATEGY: FOR A STRONGER AND MORE PROSPEROUS CANADA 3 (2010), *available at* http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf [hereinafter *Canada's Cyber Security Strategy*].

46. *See UK Cyber Security Strategy*, *supra* note 45, at 26; *Canada's Cyber Security Strategy*, *supra* note 45, at 12–13.

47. U.N. Charter art. 51.

may be impacted by the unique aspects of cyber warfare is the concept of legitimate participants in warfare. A hallmark of contemporary international law and war is the separation of the rules governing the conduct of warfare from those constraining the recourse to war.[48] While it is important to have the *jus ad bellum* considered separately from the *jus in bello* (or international humanitarian law) in order to maintain the "equal application" principle regarding the rules that govern warfare, that cannot always be easily done. This is particularly evident regarding the status of persons taking part in hostilities. The breadth of civilian involvement in the cyber domain, both inside and outside of government, will place even greater stress on traditional notions of legitimate participation in armed conflict.

One of the challenges arising from the twentieth century obsession with restricting inter-State armed conflict has been that the *jus ad bellum* has come to be associated narrowly with national self-defense. However, reflecting its roots in just war theory, the *jus ad bellum* contains a number of other fundamental principles, such as fighting for the "proper authority."[49] The application of this principle leads, at times, to a continuing interaction between *jus ad bellum* and *jus in bello* that is perhaps most obviously displayed when legitimate participation in conflict is assessed. If you fight for the "proper authority" (i.e., a State) then you are "legitimate," having both the right to participate in armed conflict and gain the protected status of prisoner of war. This legitimate status is recognized in foundational humanitarian law treaty documents.[50] In addition, while the *jus ad bellum* is traditionally viewed not as being applicable to non-international armed conflict,[51] the principle of proper authority effectively makes those mem-

48. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 3 (2d ed. 2010) ("The fundamental postulate of the *jus in bello* is the equal application of its legal norms to all Belligerent Parties, regardless of their relative standing in the eyes of the *jus ad bellum*.").

49. JAMES TURNER JOHNSON, MORALITY AND CONTEMPORARY WARFARE 30 (1999) (outlining the *jus ad bellum* principles found under positive international law as being: just cause, right or proper authority, right intention, proportionality of ends, last resort, reasonable hope of success and the aim of peace).

50. *See* Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land arts. 1–3, Oct. 18, 1907, 36 Stat. 2227; Convention (III) Relative to the Treatment of Prisoners of War art. 4.A, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.

51. Marco Sassoli, Ius ad Bellum *and* Jus in Bello—*The Separation between the Legality of the Use of Force and Humanitarian Rules to be Respected in Warfare: Crucial or Outdated?*, *in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES 241, 254 (Michael N. Schmitt and Jelena Pejic eds., 2007) ("Technically, no international *jus ad bellum*

bers of the security forces who fight for States the legitimate actors in such conflicts. It is the non-State actors whose activities are criminalized.[52]

That said, one of the realities of the cyber domain is that combatants in international armed conflict and security personnel in internal ones cannot defend all the national digital assets on their own. Those assets, and the threats posed to them, are too numerous and broadly distributed.[53] In many respects cyber activity represents a true expansion of the "home front" as an area of operations, even into the boardrooms and bedrooms of the nation. To the extent the introduction of airpower represented a kinetic means by which State-directed violence could be extended to a broad range of targets beyond national borders, cyber provides an even more expanded and in some ways more intimate threat.

As a result, many of the potential participants in this cyber war are likely not to be wearing uniforms or bearing arms, at least in the traditional sense. Due to its scope and scale, this represents a civilian involvement that appears significantly more challenging in terms of assessing its legitimacy than the contemporary controversy regarding Central Intelligence Agency personnel conducting drone strikes.[54] This leads to fundamental questions regarding the status of civilians who man the computer defenses of a State. Are they direct participants in hostilities? Do they really have to wear a uniform and be sworn into the armed forces of the State to lawfully participate in these activities? The answers may simply be that they are legitimately carrying out the responsibilities assigned to them in the same fashion as the police officers that arrested German saboteurs who had surreptitiously

---

exists concerning non-international armed conflicts, since such conflicts are neither justified nor prohibited by international law.").

52. *See* G.I.A.D. DRAPER, THE RED CROSS CONVENTIONS 14 (1958) (discussing attempts at the end of World War II to extend the provisions of the Geneva Conventions to internal conflicts and noting that "proposals giving insurgents a legal status, and consequently support, would hamper the Government in its measures of *legitimate* repression") (emphasis added).

53. Paul Ducheine, Joop Voetelink, Jan Stinissen & Terry Gill, *Towards a Legal Framework for Military Cyber Operations*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 5, at 106 ("Given the characteristics of the threats as well as the 'battlefield' . . . , governments alone are incapable of responding adequately as they are heavily dependent upon private partners such as internet providers.").

54. Andrew Burt & Alex Wagner, *Blurred Lines: An Argument for a More Robust Legal Framework Governing the CIA Drone Program*, 38 YALE JOURNAL OF INTERNATIONAL LAW ONLINE 1 (2012), http://www.yjil.org/docs/pub/o-38-burt-wagner-blurred-lines.pdf.

landed on the shores of the United States during World War II[55] or Jose Padilla when he landed in Chicago in 2002.[56] In complying with the requirements of domestic law in the performance of their duties, they are not illegitimate under international law. Nor should they be liable to foreign prosecution for doing so. Indeed, it would have been an odd result to suggest that any apprehension of the saboteurs, who in today's terminology were unprivileged belligerents, had to be carried out by United States military personnel regardless of the geographic location.

The widespread involvement of civilians in the defense of computer networks could once again put the fundamental humanitarian law principle of distinction under pressure. In this instance, it will not be the factory workers of World War II who are considered to be "quasi-combatants," but rather potentially those who maintain the integrity and security of computer networks in their everyday employment.[57] It will be difficult to say that those civilians are far away from the battlefield when the cyber conflict is occurring literally in their laps. In this respect, they are different than the third echelon civilian supply workers or strategic level intelligence analysts who often seem to get a "geographic" pass when direct participation in hostilities (DPH) is considered. Cyber participants may be harder to separate from the action that is occurring literally at their fingertips.

The International Committee of the Red Cross, in its *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, appears to avoid this issue by concentrating on computer network attacks against military systems[58] and the offensive use of cyber.[59] That *Interpretive Guidance* notes that for "remote-controlled (i.e. geograph-

55. LOUIS FISHER, NAZI SABOTEURS ON TRIAL 33–36 (2d ed. 2005) (outlining the arrest of the saboteurs).

56. *See* Donna Leinwand & Jack Kelley, *U.S. Citizen Arrested in 'Dirty Bomb' Plot*, USA TODAY (Nov. 6, 2002), *available at* http://usatoday30.usatoday.com/news/nation/2002/06/10/terror-arrest.htm

57. In seeking to justify attacks on factory workers as quasi-combatants, a practice no longer permitted under international law, one author explained:

> It is not a question of political or moral support, or even of material support in forms that could not possibly be called warlike. What justifies the deliberate attack on the people concerned is that they are engaged in work which his akin to that done by uniformed men in the field. They are helping to pass the ammunition.

J.M. SPAIGHT, AIR POWER AND WAR RIGHTS 47 (3d ed. 1947).

58. INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 48, 50 (2009) [hereinafter *Interpretive Guidance*].

59. *Id.* at 55, 68.

ically remote) missiles, unmanned aircraft and computer network attacks," the "causal relationship between the employment of such means and the ensuing harm remains direct regardless of temporal or geographical proximity."[60] The legal and practical challenge is that the symbiotic relationship between offense and defense means the two concepts cannot be readily divorced. As a result, participation in the defense of computer systems raises the specter of DPH.

The transformative nature of cyber is reflected in the example of a fifty-nine-year-old retired grandmother who was reported in a Canadian newspaper in June of 2011 to be passing on information obtained through the social media site Facebook to a NATO twitter account. The information was said to include the coordinates of Colonel Gadhafi's forces' temporary headquarters in Libya, "along with the longitude and latitude for other targets."[61] The woman lived in central Canada just north of the United States border, obviously a considerable distance from the Libyan battlefield.[62] Another person passing on details regarding fuel tankers at a Libyan port was reported to be a forty-eight-year-old ice cream business supervisor in Arizona.[63] Is a person who takes information posted by someone else from the web and passes it on taking a direct part in hostilities? The *Interpretive Guidance* makes a link between the transmittal of tactical intelligence and the potential causation of harm resulting from any targeting decision.[64] Scenarios such as these raise questions of degrees of remoteness and where the line will be drawn on cyber DPH.[65]

In any event, so what if civilians are involved in cyber conflict? Such participation is not illegal under international humanitarian law unless it engages issues of perfidy, although some activity does theoretically raise

---

60. *Id.* at 55.

61. Graeme Smith, *How social media users are helping NATO fight Gadhafi in Libya*, GLOBE AND MAIL (Canada) (June 14, 2011), *available at* http://www.theglobeandmail.com/news/world/how-social-media-users-are-helping-nato-fight-gadhafi-in-libya/article583325/.

62. *Id.*

63. *Id.*

64. *Interpretive Guidance*, *supra* note 58, at 54–55 ("More precisely, where a specific act does not on its own directly cause the required threshold of harm, the requirement of direct causation would still be fulfilled where the act constitutes an integral part of a concrete and coordinated tactical operation that directly causes such harm.").

65. Smith, *supra* note 61 (noting "[a] Twitter account with apparent links to the British military has even taken the unusual step of asking users to submit the precise co-ordinates of troops loyal to Colonel Moammar Gadhafi").

questions of prosecution under the domestic jurisdiction of an opposing State if a participant is ever captured.[66] It also does not mean there could not be other potential consequences. For example, the operators of unmanned drones are located in the United States and the strikes are occurring in Afghanistan, Iraq and elsewhere on the other side of the globe.[67] Cyber connectivity means, however, that direct participants may be subjected to a cyber response, although likely one leading to a denial-of-access or disabling of means rather than one that is destructive in nature.

If it is not participants themselves, then the State in which they are operating may draw the attention of the targeted State. This is not necessarily problematic when that State itself is already a belligerent in the armed conflict. However, for the States that conducted the bombing campaign in Libya, it might have come as a shock if a cyber response from the government of Libya had been directed at them from so far away. In other situations where the State has no intentions of being a belligerent, the global nature of cyber has the potential to engage the responsibility of States for activities emanating from their territory much more broadly and swiftly than in the past. For example, it is reported that when it was subjected to distributed-denial-of-service (DDoS) attacks against its websites during the 2008 conflict with Russia, Georgia transferred official Internet assets to the United States, Estonia and Poland.[68] This has raised questions regarding United States neutrality. In this respect, "[t]he fact that American IT companies provided assistance to Georgia, a cyber belligerent, apparently without the knowledge or approval of the U.S. government, illustrates what is likely to become a significant policy issue."[69]

---

66. *See* ALLAN ROSAS, THE LEGAL STATUS OF PRISONERS OF WAR: A STUDY IN INTERNATIONAL HUMANITARIAN LAW APPLICABLE IN ARMED CONFLICT 305 (1976) (explaining that a person not having the status of lawful combatant "may be punished under the internal criminal legislation of the adversary for having committed hostile acts in violation of its provision (e.g. for murder), even if these acts do not constitute war crimes under international law"). *See also* DINSTEIN, *supra* note 48, at 35–39 (discussing the consequences of unlawful combatancy).

67. *See* Elizabeth Bumiller, *A Day Job Waiting for a Kill Shot a World Away*, NEW YORK TIMES, July 30, 2012, at A1, *available at* http://www.nytimes.com/2012/07/30/us/drone-pilots-waiting-for-a-kill-shot-7000-miles-away.html?pagewanted=all; MATT J. MARTIN, PREDATOR REMOTE-CONTROL AIR WAR OVER IRAQ AND AFGHANISTAN: A PILOT'S STORY 30 (2010).

68. Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERS, Winter 2008, at 60, 60.

69. *Id.* at 61.

If civilian participation in cyber warfare from either an offensive or defensive perspective is seen as problematic, what is the true role for those in uniform and those who wear more casual attire? Given the nature of the medium, the scope of the activity and the importance of the information, it appears that international lawyers are not going to easily put such "unprivileged" participation back in the traditional combatant box. And given this interface with citizens on the domestic front, the discussion inevitably will not be just about the separation of *jus ad bellum* and *jus in bello*, or who can fight or not, but also domestic privacy, criminal law, and human and civil rights. This ultimately will require a more holistic application of the law impacting on operations. Perhaps this requirement to consider the broader implications of cyber conflict will force an application of operational law spanning numerous legal disciplines rather than deal with the issues compartmentalized into traditional legal silos.[70]

International lawyers are also going to have to be prepared to explain to a varied group of colleagues, both lawyers and non-lawyers, why combatant status matters in a cyber conflict with global reach but tangible domestic impact. It also means that some military lawyers, whose area of expertise may be limited to the law of armed conflict, will need to become much better acquainted with the impact *jus ad bellum*, international human rights law and domestic law have on cyber operations. At a minimum, it will present a daunting educational, training and doctrinal challenge for many military and civilian government legal advisors.

B. An "Armed" Attack: Really?

1. Cyber Weapons and Effects

Notwithstanding the requirement to come to grips with the breadth of civilian participation in cyber operations, perhaps the greatest challenge for international lawyers will be to identify when cyber attacks reach the threshold necessary for a State to legitimately respond in self-defense.[71]

---

70. *See* Headquarters, Department of the Army, FM 1-04, Legal Support to the Operational Army ¶ 5-4 (2012) (Operational law is "the body of domestic, foreign, and international law that directly affects the conduct of military operations."); *see also* Office of the Judge Advocate General, Roles and Responsibilities (2012) (defining "operational law" as "that body of domestic and international law that applies to the conduct of all phases of a CF operation at all levels of command").

71. UN Charter art. 51.

With international law indicating "it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms" the international legal community has struggled with identifying the gravity threshold.[72] The mining of a warship might meet that threshold,[73] but mere frontier incidents would not.[74] Given this lack of consensus regarding kinetic uses of force, it is likely cyber attacks will present an even greater challenge.

To even begin to address that issue, there first must be an understanding that a computer is potentially a weapon. In a legal context, a weapon is assessed both as a means and method of warfare that is of a nature to cause superfluous injury or unnecessary suffering.[75] However, the nature of the challenge is perhaps most clearly framed in non-legal terms. A weapon has been defined as: "a thing designed or used for inflicting bodily harm or physical damage: *nuclear weapons*."[76]

This concept of weapon creates two challenges in the cyber domain. The first is the need to convince the broader public that computers (the laptops, desktops, tablets and even phones carried by much of the public, including, no doubt, committed pacifists) are, in fact, weapons like rifles, artillery and fighter aircraft. Of course, as was tragically demonstrated during the genocide in Rwanda, even basic implements such as knives and machetes can be turned into an instrument of mass death.[77] However, the issue is whether the ubiquitous computer, which requires a certain level of sophistication to operate, but does not project a shell or offer much in the way of being a blunt instrument, could also be used as a weapon in its own right.

---

72. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 191 (June 27) [hereinafter *Nicaragua*].

73. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 72 (Nov. 6) ("The Court does not exclude the possibility that the mining of a single military vessel might be sufficient to bring into play the 'inherent right of self-defence'. . . ."); *See also* Waxman, *supra* note 44, at 438 (indicating the United States argued successfully for a low Article 51 threshold.).

74. *Nicaragua*, supra note 71, ¶ 194.

75. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 37, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

76. OXFORD DICTIONARIES ONLINE, *supra* note 12 (emphasis added).

77. SAMANTHA POWER, "A PROBLEM FROM HELL": AMERICA AND THE AGE OF GENOCIDE 334 (2002) (outlining how the genocide started with the use of firearms, but as it spread throughout Rwanda the weapons became "increasingly unsophisticated—knives, machetes, spears and the traditional masu, bulky clubs with nails protruding from them").

Second, there must be an acceptance that cyber means can inflict bodily harm or physical damage. This is an area where determining the *lex lata* (what the law is) for the *jus ad bellum* has been particularly challenging. It has led to efforts to assess the "effects" generated by a computer by an analogy to kinetic weapons. Among the questions being debated is whether computer attacks should be looked at using an instrument-based approach (i.e., one that produces equivalent results to a kinetics-based attack) in assessing whether such an attack can reach the level of an armed attack under Article 51 of the UN Charter.[78] However, the conceptual and legal path connecting the pressing of a computer key to ultimately causing a destructive effect approaching that of an armed attack is anything but straightforward. It might be analogized to the bombing of a dam gate thereby releasing floodwaters. As the Stuxnet attack has demonstrated, physical damage can occur. That is not the only way that cyber operations can lead to physical damage, death or injury. For example, a cyber penetration of a SCADA system could be considered the same as a covert insertion of a Special Forces team, which, after gaining access to the control facility, turns the dial opening the gates. While such activity might constitute an armed attack, the overall analysis would benefit by not jumping to a bullets and bombs (i.e., kinetic) approach.[79]

Another method for considering what constitutes an armed attack is the effects-based approach, i.e., whether it produces severe enough effects that it warrants treatment as an armed attack. Jeffrey Carr provides the example of an armed attack in which one party "manipulated information across a state's banking and financial institutions to seriously disrupt commerce in the state."[80] This approach does not try to equate the use of cyber

---

78. An instrument-based approach is described as

> a cyber attack used to shut down a power grid is an armed attack. This is because shutting down a power grid typically required dropping a bomb on a power station or some other kinetic use of force to incapacitate the grid. Since conventional munitions were previously required to achieve the result, under the instrument-based approach the cyber attack is therefore treated the same way.

CARR, *supra* note 1, at 59

79. YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 212 (5th ed. 2011) ("If CNA [computer network attack] were to cause severe damage to property or even human fatalities (as a result, e.g., of the shutdown of computers controlling waterworks and damns, leading to the flooding of inhabited areas), it would qualify as an armed attack.").

80. An effects-based approach is described as

to a kinetic attack, but rather seeks to assess the quantum of loss in an economic sense. The challenge here is twofold. First, as has been noted, international law has struggled with the very notion of categorizing loss in a kinetic context. It is not clear how this approach will add any greater clarity. Second, the effects-based approach appears to involve a particularly commercial calculus.

It is not clear where the separation is between loss, damage, disruption, theft and simple espionage with regard to the ability to conduct commerce. Further, given the nature of international commercial relations, it is not clear whether this approach only involves attacks on nationally owned or based corporations, international corporations and their subsidiaries, private financial institutions, e.g., Wall Street, or institutions more closely associated with the State, such as the Federal Reserve in the United States.

What this approach does do is highlight that the basis for an armed attack has always included an economic component. For example, the establishment of a blockade by one State against another, albeit with the threat of military force backing it, could be seen as an armed attack justifying a response in self-defense.[81] It is not clear, however, that the likely means of a cyber blockade, a DDoS attack, even falls under the effects-based approach or equates to a use of force under Article 2(4) of the Charter? It must constitute a use of force before it can be considered as an armed attack.

This raises the question of whether the use of force under Article 2(4) is broader than simply armed force extended to economic matters. Such an interpretation is one that most Western economically powerful States and international lawyers have resisted, although "developing countries and formerly the Eastern bloc countries have repeatedly claimed that the prohibition on the use of force also comprises other forms of force, for instance, political and, in particular, economic coercion."[82]

> a cyber attack that manipulated information across a state's banking and financial institutions to seriously disrupt commerce in the state is an armed attack. Although the manipulation of information does not resemble a kinetic attack, as required under an instrument-based approach, the disruptive effects that the attack had on the state's economy is a severe enough overall consequence that it warrants treatment as an armed attack.
>
> CARR, *supra* note 1, at 59

81. Albrecht Randelzhofer, *Article 51*, *in* 1 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 788, 797 (Bruno Simma ed., 2d ed. 2002).

82. Albrecht Randelzhofer, *Article 2(4)*, *in id.* at 112, 118. *See also* CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 30 (3d ed., 2008) ("There is a split be-

Malcolm Shaw notes this issue was considered in the past in "light of the Arab oil weapon used in 1973-4 against States deemed favorable to Israel."[83] While he indicates there is a case to be made that such actions are contrary to the Charter, ultimately "whether such action constitutes a violation of Article 2(4) is dubious."[84] The prevailing view is that economic coercion would not qualify as a use of force under Article 2(4), let alone form the justification for acting in self-defense under Article 51.[85] In this respect it has been noted, "were this provision [Article 2(4)] to extend to other forms of force, States would be left with no means of exerting pressure on other States that violate the law."[86] This is an important issue when considering the use of cyber means in the form of countermeasures.

Given this background, an effort by economically powerful States, such as the United States, that have computer-based economies to now widen the basis for reaction in self-defense by including the economic impact of computer activity as an armed attack could have unintended consequences if it results in a broadening of Article 2(4) to include economic coercion. This is not to suggest it should not be done, but in doing so a careful analysis needs to be undertaken that looks beyond the narrow interests of the more technologically advanced States. At the same time, it would also be ironic if less economically developed States, which might also have less advanced cyber capabilities, embraced an argument that such "economic" focused uses of cyber were not an armed attack under international law because of the asymmetric advantage they now might have.

---

tween developed and developing states as to whether 'the use of force' includes not only armed force but economic coercion."); Waxman, *supra* note 44, at 428–29.

83. SHAW, *supra* note 32, at 1125. *See also* 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), *reprinted in* ESSAYS ON LAW AND WAR AT THE FAULT LINES 3, 24 (Michael N. Schmitt ed., 2012) ("Because the results of applying economic and political instruments constitute lesser threats to shared community values, the use of force standard serves as a logical break point in categorizing the asperity of particular coercive acts.").

84. SHAW, *supra* note 32, at 1125.

85. *See* DINSTEIN, *supra* note 79, at 88 ("[W]hen studied in context, the term 'force' in Article 2(4) must denote violence. It does not matter what specific means—kinetic or electronic are used to bring it about, but the end result must be that violence occurs or is threatened. Therefore, psychological or economic pressure (e.g. in the form or economic boycott) as such does not come within the purview of the Article, unless coupled with the use or at least the threat of force."); Schmitt, *supra* note 83, at 22.

86. Randelzofher, *supra* note 82, at 118.

2. Cyber and Force

Of course, even before there is a discussion of armed attack there must be acceptance that there is a use of force.[87] There is an interpretation of the law developed in 1999 by Michael Schmitt that cyber specific criteria, e.g., severity, immediacy, directness, invasiveness, measurability and presumptive legitimacy, could be applied to assess if a use of force has occurred.[88] These criteria appear to fall well within the concept of *lex ferenda*, or what the law ought to be. Indeed, the 2013 *Tallinn Manual*, a project in which this author participated, indicates the criteria are not to be viewed as formal legal requirements, but rather as factors "that influence States making use of force assessments."[89]

Of note, these factors are set out in the *Manual* commentary rather than the rules.[90] In the *Tallinn Manual*, it is stated the rules "reflect consensus among the Experts as to the applicable *lex lata*, that is, the law currently governing cyber conflict. It does not set forth *lex ferenda,* best practice, or preferred policy."[91] The commentary is "intended to identify its legal basis, explain its normative content, address practical implications in the cyber context, and set forth differing positions as to scope or interpretation."[92] The fact that the *lex lata* in this instance is justified by such extensive reference to relatively recent interpretations of the law, even if it was only in the context of taking note of the theory, stands out as an example of the challenge presented by cyber warfare.[93] The technology is new, indeed cutting

87. For an excellent discussion of Article 2(4) in the cyber context, see Waxman, *supra* note 44.

88. Schmitt, *supra* note 83, at 26.

89. TALLINN MANUAL, *supra* note 4, rule 11, ¶ 9.

90. *Id.*, rule 11, ¶¶ 8–11.

91. *Id.* at 19.

92. *Id.* at 20.

93. The *Tallinn Manual* explains the rationale for using these criteria as follows:

> Acts that injure or kill persons or damage or destroy objects are unambiguously uses of force (see commentary to Rule 13 expressing an analogous conclusion, but requiring the harm to be 'significant'). Since other cases are less clear, the International Group of Experts took notice of an approach that seeks to assess the likelihood that States will characterise a cyber operation as a use of force. The method expounded operates on the premise that in the absence of a conclusive definitional threshold, States contemplating cyber operations, or that are the target thereof, must be highly sensitive to the international community's probable assessment of whether the operations violate the prohibition on the use of force.

edge, but the established law is "old" law, which is, in many ways, retrospective to the immediate post-World War II era.

What adopting these factors would mean is an acceptance of a dual threshold for assessing force and cyber operations. In this respect, the *Tallinn Manual* indicates "[a] cyber operation constitutes a use of force when its *scale and effects* are comparable to non-cyber operations rising to the level of a use of force."[94] Similarly, "[w]hether a cyber operation constitutes an armed attack depends on its *scale and effects*."[95] The *Manual* relies on the same interpretation of the *Nicaragua* decision to explain the use of the term "scale and effect" as the basis for assessing both the use of force[96] and armed attack.[97] However, "[t]he scale and effects required for an act to be characterised as an armed attack necessarily exceed those qualifying the act as a use of force."[98]

While this is a sound interpretation of widely accepted principles of international law as it has developed to date, it is not clear how well this standard will be applied in practice. A majority of the experts writing the *Manual* were reported to have believed "the critical factor was whether the effects of a cyber operation, as distinct from the means used to achieve those effects, were analogous to those that would result from an action otherwise qualifying as a kinetic armed attack."[99] This suggests an instruments-based approach, although the scale-and-effects argument arguably fits more comfortably with the effects-based approach. There is a degree of overlap between both approaches in that one of the factors that often points to a kinetic armed attack is the tangibly measurable effects created by that violence.

The instruments-based approach appears to be the one favored by the United States Government for assessing if a use of force has occurred. As was indicated by the U.S. State Department Legal Advisor Harold Koh in September 2012, "if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would,

---

Id., rule 11, ¶ 8 (citation omitted).
94. *Id.*, rule 11 (emphasis added).
95. *Id.*, rule 13 (emphasis added).
96. *Id.*, rule 11, ¶ 1.
97. *Id.,* rule 13, ¶ 6.
98. *Id.,* rule 13, ¶ 5.
99. *Id.,* rule 13, ¶ 4.

that cyber attack should equally be considered a use of force."[100] Of note, these references were made with respect to meeting the basic threshold of a use of force. Mr. Koh also reiterated the United States' position that "there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response."[101] While this continues to place the United States in an outlier position in relation to the broader international community regarding the legal basis for acting in self-defense, there is little chance that a cyber context would have changed this approach given the general lack of consensus regarding what constitutes a use of force in that domain. That said, the United States, or any other State that takes this position, will still need to identify the threshold for a use of force at which point a response in self-defense would be justified.

Further, it is not clear if any message can be taken from the fact that the examples provided—the causing of a nuclear plant meltdown, opening dam doors and disabling air traffic control—did not include an attack on the financial markets.[102] Its omission may simply reflect what conceptually difficult issues such an attack poses for traditional international law. These examples also do not clearly establish the minimum threshold upon which action is considered justified. Further, it was noted that "there are other types of cyber actions that do not have a clear kinetic parallel, which raise profound questions about exactly what we mean by 'force.'"[103]

The *Tallinn Manual* does address attacks on financial institutions; however, the commentary discussion of what is described as the "classic scenario" of an attack on the New York Stock Exchange reflected quite divided opinions that go to the heart of the discussion of regulating force in the cyber domain.[104] There is a danger that the reference to the New York Stock Exchange shows a Western and, in particular, U.S. concern with interference with commerce. An interesting issue is whether disruption of the

---

100. Harold Koh, Legal Advisor, U.S. Department of State, Remarks at USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *available at* http://www.state.gov/s/l/ releases/remarks/197924.htm [hereinafter *Koh Remarks*].

101. *Id. See also* Sean D. Murphy, *U.S. Reaction to ICJ Judgment in Iranian Oil Platforms Case*, 98 AMERICAN JOURNAL OF INTERNATIONAL LAW 597 (2004).

102. *Koh Remarks*, *supra* note 100.

103. *Id.*

104. TALLINN MANUAL, *supra* note 4, rule 13, ¶ 9 ("Some of the Experts took the position that harm to persons or physical damage to property is a condition precedent to the characterisation of an incident as an armed attack. Others took the view that it is not the nature (injurious or destructive) of the consequences that matters, but rather the extent of the ensuing effects.").

Shanghai, Tokyo or London stock exchanges would garner the same concerns. Further, given the interconnected nature of the financial markets, if there was an attack on one of these other exchanges could another State claim it was an attack on their economic interests, if they were adversely impacted collaterally, even though the State hosting the targeted exchange did not share the view? This lack of consensus and the unclear theoretical underpinning for such activity to be called an armed attack suggests caution is required in coming to any conclusions at this stage.

There is a significant danger in overstating the effects of cyber attacks even when they impact on infrastructure such as dams, power generation facilities or other utilities. Again it may be helpful to return to the Y2K experience. Notwithstanding dire predictions regarding potential failures of SCADA and other computerized systems controlling pipelines, electrical grids, trains and even weapon systems,[105] a study of many of these systems at the time of Y2K demonstrated they were quite resilient. As the *United States Y2K Study* indicated, critical industries "include a great deal of competing systems created by deregulation and technological advancements in recent decades."[106] A particular exception was the electrical power distribution network; however, even here there was substantial redundancy.[107] As that study noted in its discussion of critical infrastructure, "[i]n an economy as large as the United States, hundreds and perhaps thousands of failures in 'critical infrastructure' electricity or water systems could occur before the impact would be great enough before there would be a significant impact."[108]

Another challenge in assessing the impact of cyber operations is that the infrastructure itself may be particularly vulnerable to being adversely affected by other factors unrelated to the intensity of the cyber activity. In other words a piece of malware may not, on its own, be a use of force or an attack, although its presence may have unintended consequences. It is reported that in 2003, fifty million people were out of power in the eastern United States and central Canada because a falling tree created a surge in a power line that apparently slowed back up controls, in part, because of a software glitch and computer malware.[109] In situations such as this, sorting out the responsibility for the actual blackout may be difficult to ascertain.

105. CLARKE & KNAKE, *supra* note 14, at 96–101.
106. *United States Y2K Study*, *supra* note 15, at 23.
107. *Id.*
108. *Id.* at 7.
109. CLARKE & KNAKE, *supra* note14, at 99.

One challenge appears to be the relative reliability and robustness of the power grid. For example, a former Energy Secretary in the United States noted notwithstanding U.S. military and economic might has

> a grid that is antiquated, that is Third World, that needs beefing up. We've got very weak power transmission lines and generation capacity. That's because there hasn't been investment in our electricity grid because there's been no competition, because there's been a lot of monopoly control of utilities in this country.[110]

Not only does there need to be further study to gather the facts, the legal community should reach out to other disciplines to become better informed before embracing the notion that a cyber-induced power failure generally provides the threshold for the existence of an armed attack.

Another factor to be considered in assessing the scale and effects of cyber operations is that many populations have shown themselves to be quite resilient when confronted with either man-made or natural disasters. This has included significant power failures or blackouts affecting millions of persons both within a country and extending across borders. In addition to the above-mentioned 2003 North American incident, significant blackouts have occurred in Europe in 2006[111] and more recently in India in 2012.[112] Some disruptions have occurred in inhospitable climates, such as in Canada as a result of an ice storm during the winter of 1998[113] and in the

---

110. Interview with Bill Richardson, former U.S. Secretary of Energy, Frontline, PBS (Apr. 10,2001), http://www.pbs.org/wgbh/pages/frontline/shows/blackout/interviews/richardson.html.

111. Stephen Castle, *Europe suffers worst blackout for three decades*, THE INDEPENDENT (Nov. 6, 2006), http://www.independent.co.uk/news/world/europe/europe-suffers-worst-blackout-for-three-decades-423144.html# ("The power loss came about when Germany's network became overloaded, probably as a result of a routine shut down of a high-voltage transmission line under the Ems river to allow a ship to pass by safely. The fallout from the incident, said to be one of the worst since the 1970s, left engineers and politicians aghast, and underlined the interdependence of European countries' electricity grids.").

112. *India blackouts affect half the country*, CBC NEWS (July 31, 2012), http://www.cbc.ca/news/world/story/2012/07/31/india-power-outage.html ("Its impact, however, was softened by Indians' familiarity with frequent blackouts and the widespread use of backup generators for major businesses and key facilities such as hospitals and airports.").

113. Eric Harris, *Struck Powerless*, CANADIAN GEOGRAPHIC, Mar.–Apr. 1998, *available at* http://www.canadiangeographic.ca/magazine/ma98/feature_ice_storm.asp.

United States in 2009.[114] Given that States deal with these types of challenges on a fairly regular basis, this may inoculate their societies from rushing to a conclusion that cyber events leading to SCADA interference should be viewed as such a threat to national security that going to war is warranted.

As a result, to take the position that cyber activity causing a power failure generally establishes the threshold for an armed attack, or even constitutes a use of force permitting an armed response if the United States position is applied, could be problematic. Without developing a generally agreed to scale-and-effects assessment of the actual, or even potential, impact of such cyber activity a State could embark down a course leading to an armed conflict involving not only wider cyber attacks, but also kinetic violence.

It may be that the international law standard of a grave use of force justifying action in self-defense may not readily translate in equivalency to the effects of a power failure that is not exceptionally disruptive to the overall functioning of the economy of a State, or cause a substantial loss of life.[115] The question from an *ad bellum* perspective is at what point effects that can also be caused by human frailty or weather should be equated to an armed attack, such that they justifiably prompt a response that could result in two or more nations going to war.

That is not to say that interference with SCADA systems could not reach the threshold of an armed attack if you apply a scale-and-effects approach. Not all cyber-induced failures of power and other industries would necessarily reach that threshold, however. Indeed, there is some skepticism that a purely cyber war will ever develop that would be "violent, instrumental, and—most importantly—politically attributed."[116]

---

114. *See Ice Storm Cuts Power Throughout Northeast*, CBS NEWS (Feb. 11, 2009), http://www.cbsnews.com/2100-201_162-4665303.html.

115. CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 4, at 119 (referencing an advisor report for the Dutch government that indicated that where there is a cyber attack to leading to "a *significant* number of fatalities or causes *substantial* physical damage or destruction to vital infrastructure, military platforms or installations or civil property, it could certainly be qualified as an 'armed attack'") (emphasis added).

116. Thomas Rid, *Cyber War Will Not Take Place*, 35 JOURNAL OF STRATEGIC STUDIES 5, 29 (2012).

3. Countermeasures

A real advantage of cyber operations is that much of the activity occurs outside of the public eye at a micro level not normally associated with armed conflict. This presents two types of opportunities for a State. One is to covertly engage in activity that reaches the level of a use of force or an armed attack and rely on such activity not being discovered or attributed to that State.[117] Such activity is problematic from an international law perspective. Another advantage of this new technology is that it provides a means for a State to act in response to threats without crossing the armed conflict threshold. In effect, it is one of the means by which wider and more violent conflict can be avoided in the first place. When the cyber activity amounts to an internationally wrongful act, there are options short of war for responding to threats under the international legal system. The problem is that those responses are often excluded—or at least pushed into the background—in the contemporary dialogue regarding operations in the cyber domain which appears to focus on force.

There is the very real danger that focusing discussion on the less likely occurrence of armed attack will overshadow the potential use of cyber in other circumstances. In this regard a cyber weapon might be thought of in less bellicose terms by considering it in the context of the rest of the Oxford definition: "a means of gaining an advantage or defending oneself in a conflict or contest: *resignation threats had long been a weapon in his armoury*."[118]

Perhaps a primary function of cyber is more accurately considered as a weapon of a different sort, one divorced from those producing kinetic results. Cyber should not necessarily be seen as having a violence-producing capability at the level of an armed attack—or even a use of armed force. Instead, it is simply a use of force, or maybe not even that. Cyber activities have the potential to offer a non-violent means to sanction a State for its internationally wrongful act as countermeasures.[119]

---

117. Arquilla, *supra* note 42 ("The culprit is the bits and bytes that are the principal weapons of cyberwar. It is now possible to intervene swiftly and secretly anywhere in the world, riding the rails of the global information infrastructure to strike at one's enemies. Such attacks can be mounted with little risk of discovery, as the veil of anonymity that cloaks the virtual domain is hard to pierce. And even when 'outed,' a lack of convincing forensic evidence to finger the perpetrator makes heated denials hard to disprove.").

118. OXFORD DICTIONARIES ONLINE, *supra* note 12 (emphasis added).

119. *Nicaragua, supra* note 71, at 106, ¶ 201 ("[T]he Court must enquire whether there is any justification for the activities in question, to be found not in the right of collective

The *Tallinn Manual* addresses countermeasures in Rule 9, which states "[a] State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State."[120] A widely held view is that countermeasures cannot involve the use of armed force.[121] Countermeasures are exceptional in that they may justify otherwise unlawful conduct taken in response to a previous intentionally wrongful act of another State.[122] In this respect, they are different than retorsion, which is a response by means of an "unfriendly act not amounting to a violation of international law, to either (a) a breach of international law or (b) an unfriendly act, by another State."[123] Retorsion can include breaking off diplomatic relations, discontinuing or withholding of trade, denying economic or financial benefits, etc.[124] Importantly, acts of retorsion can involve cyber measures, such as occurred when Estonia "suspended some services to internet protocol (IP) addresses from Russia."[125]

The concept of countermeasures is a broad one with reference sometimes being "made to the application of a 'sanction' or to a 'reaction' to a prior internationally wrongful act; historically the more usual terminology was that of 'legitimate reprisals' or, more generally, measures of 'self-protection' or 'self-help.'"[126] Countermeasures "are essentially temporary measures, taken to achieve a specified end, whose justification terminates once the end is achieved."[127] The wide range of permissible non-forcible actions is reflected, in part, in Article 41 of the UN Charter in its reference to "measures not involving the use of armed force," including "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of

---

self-defence against an armed attack, but in the right to take counter-measures in response to conduct of Nicaragua which is not alleged to constitute an armed attack.").

120. TALLINN MANUAL, *supra* note 4, rule 9.

121. *See* DINSTEIN, *supra* note 79, at 209.

122. Draft Articles on Responsibility of States for Internationally Wrongful Acts art. 22, ¶ (2), at 75, Rep. of the Int'l L. Comm'n, 53d Sess., UN GAOR 56th Sess., Supp. No. 10, at 181, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2), *available at* http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [hereinafter *Draft Articles on State Responsibility*]

123. ANTONIO CASSESE, INTERNATIONAL LAW 310 (2d ed. 2005).

124. *Id.*

125. TALLINN MANUAL, *supra* note 4, rule 9, ¶ 13.

126. *Draft Articles on State Responsibility*, *supra* note 122, art. 22, ¶ (3), at 75.

127. *Id.*, ch. II cmt. ¶ (4), at 129.

diplomatic relations." This article specifically endorses economic coercion, although only when decided by the Security Council.[128] That being said, these measures are reflective of the types of countermeasures and acts of retorsion that might be contemplated since they are viewed as not involving the use of armed force.

The reference to measures involving economic coercion further highlights that rushing too quickly to include the disruption of commerce under the scope of a cyber armed attack may actually restrict policy and operational options available to technologically advanced States. Those States must, however, be prepared to confront a more level cyber playing field with traditionally less capable States, which respond to advanced State activities by interfering with their economies. Economically powerful States might, however, have a very low threshold of acceptance for such activity.

The debate over cyber countermeasures may also cause a reconsideration of whether such measures can involve the use of force that falls below the level of armed attack. Judge Simma, in his separate opinion in the *Oil Platforms* case, concluded that countermeasures "[a]gainst such smaller scale use[s] of force, defensive action—by force also 'short of' Article 51—is to be regarded as lawful."[129] Such an approach garnered the support of other respected academics, although this view of the law has remained a minority one.[130] However, it may be preferable to allow more limited cyber exchanges between potential antagonists than force the confrontation into the realm of self-defense and ultimately armed conflict. The challenge when using computer network operations as a countermeasure is to ensure that the response remains below the threshold of an armed attack. This requires an ability to identify and articulate where on the gravity scale such a cyber use of armed force will lie, which has proven difficult to identify.[131] The

128. W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION 28 (1992).

129. *See* Oil Platforms*, supra* note 73, at 332, ¶ 12 (separate opinion of Judge Simma).

130. *See* CASSESE, *supra* note 123, at 371–72; THOMAS M. FRANCK, RECOURSE TO FORCE: STATE ACTION AGAINST THREATS AND ARMED ATTACKS 109–112 (2002) (recognizing the right to use force measures in response to attacks below the threshold of "armed attack."). *But see* LINDSAY MOIR, REAPPRAISING THE RESORT TO FORCE: INTERNATIONAL LAW, *JUS AD BELLUM* AND THE WAR ON TERROR 29 (2010) (noting that other commentators have taken the view "any such activities were violations of the *jus ad bellum*").

131. *See* REISMAN & BAKER, *supra* note 128, at 28 (noting that the language of some United Nations resolutions "prohibits only grave forms of coercion without indicating

legal assessment of the gravity of an attack has not been made any easier by the terminology that is commonly employed with respect to such cyber activity. It is that issue to which the analysis will now turn.

4. Terminology: The Impact of Words

It may very well be that the dialogue of cyber is pushed into the force realm by the terminology that has been applied to describe cyber activity. The most obvious examples are the terms "computer network *attack*"[132] and "computer network *defense*."[133] However, it is also evident in the national cyber security policy of Canada, which extends the concept of cyber attack to unintentional access to and use of information.[134] The use of the term "attack" invokes a perception of military activity, but in reality the cyber activity may simply involve limited manipulation of information.

A downside of lawyers entering the cyber highway so late is that there has not been an opportunity to help select the terms used to describe cyber operations. While the operational, doctrinal and legal communities use the same words, those words do not always have the same meaning. The use of the warlike term "attack" for an exceptionally broad range of computer activity is fraught with the potential for misunderstanding and overreaction that can have significant consequences, particularly at a strategic level. A political leader or media outlet may rightly claim, from a doctrinal perspective, that a "computer network attack" has taken place when another State is alleged to have hacked into the data-storage system and stolen sensitive

---

where and how minor economic coercion becomes grave"). *See also* Waxman, *supra* note 44, at 429.

132. "Computer network attack" is defined as "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA." Joint Chiefs of Staff, Joint Publication 1-02, DOD Dictionary of Military and Associated Terms (Nov. 8, 2010), as amended through July 15, 2012, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

133. "Computer network defense" is defined as "[a]ctions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. Also called CND." *Id.*

134. *Canada's Cyber Security Strategy*, *supra* note 45, at 3 ("Cyber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security.").

information relating to a defense procurement project.[135] That statement could create the perception that there was an act of force inflicted by one State on another, when the "attack" simply involved the destruction of information on a computer or was conducted as a step precedent to an act of espionage. The real challenge for many States is that they are themselves engaged in the same activity.[136] Calling such activity an attack could make it easier for other States to characterize what is, in effect, espionage as illegitimate. This could be exceptionally counterproductive for the State subjected to the espionage when the issue is assessed from a broader strategic perspective.[137]

The gap in meaning between a computer network attack and even the low threshold of a use of force under the *jus ad bellum* highlights the risks inherent in not adopting a commonly acceptable language to describe activities in the cyber domain. Significantly, the use of terms like attack also potentially limits non-forceful responses, since even the most basic penetration of a computer network appears to engage some aspect of computer network attack. For example, a State may be reluctant to use cyber means to respond to incidents out of concern relatively minor cyber activity can be mischaracterized as a more aggressive action potentially justifying a kinetic response by the aggrieved State.

There is terminology from the criminal sphere, such as "illegal access," "illegal interception," "data interference," "misuse of devices," "computer related forgery" and "computer related fraud" found in the Council of Europe's Convention on Cybercrime that may more clearly define most cyber activity and provide less opportunity for misunderstanding and confusion.[138] It is noteworthy that the use of terms such as attack was avoided in the convention, although attacks are referred to in its accompanying ex-

---

135. CLARKE & KNAKE, *supra* note 14, at 233–35.

136. *Id.* at 235 ("The ways in which we collect information, including by cyber espionage, may offend some people's sensibilities and may sometimes violate international or national laws, but, with some notable exceptions, U.S. espionage activities are generally necessary and beneficial to U.S. interests.").

137. *Id.* (noting that even entering into a treaty to limit such activity would be problematic from a national security perspective).

138. Council of Europe, Convention on Cybercrime arts. 2–6, Nov. 21, 2001, E.T.S. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; Paul A. Matus, *Strategic Impact of Cyber Warfare Rules for the United States* 10–13, 31–2 (2010), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA522001

planatory report.[139] What is not clear is how easy it would be at this stage to alter the attack terminology that may have become entrenched in national security doctrine. But the use of terms focused on criminal activity, when that in fact is what is being described in such doctrine, would help avoid confusion and misunderstanding regarding the nature of the cyber threat from a national defense perspective.

In many respects, terminology in the non-legal world has shown itself to be more subject to change than its legal counterpart. Perhaps one of the best examples of the fluidity of terminology can be found in the efforts to describe guerrilla warfare. In this regard, a myriad of terms have been applied to such conflicts, including "small wars,"[140] "imperial policing,"[141] "police action,"[142] "insurgency,"[143] low intensity conflict,"[144] "military operations other than war,"[145] "peacekeeping,"[146] "peace enforcement,"[147] three

139. Council of Europe, Committee of Ministers, Convention on Cybercrime, Explanatory Report (Nov. 8, 2001), *available at* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm .

140. *See* C.E. CALDWELL, SMALL WARS: THEIR PRINCIPLES AND PRACTICE 21 (3d ed. 1996); MAX BOOT, THE SAVAGE WARS OF PEACE: SMALL WARS AND THE RISE OF AMERICAN POWER xiv (2002).

141. *See* MAJOR-GENERAL SIR CHARLES W. GWYNN, IMPERIAL POLICING 3–4 (1934).

142. *See* Josef L. Kunz, *The Chaotic Status of the Laws of War and the Urgent Necessity for Their Revision,* 45 AMERICAN JOURNAL OF INTERNATIONAL LAW 37, 54 n.41 (1951) (citing P.C. Jessup, A MODERN LAW OF NATIONS 188–89 (1948) ("It is a mistake to assume that the acceptance of the concept of an international police force . . . with its subsequent abolition of the concept of 'war' in a legal sense, eliminates the necessity for the legal regulation of the rights and duties of those who are active participants in the struggle.").

143. *See* Headquarters, Departments of the Army and Air Force, FM 100-20/AFP 3-20 Military Operations in Low Intensity Conflict (1990), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB63/doc4.pdf (superseded by FM 3-07 (2003), which in turn was replaced in 2008).

144. *Id.*

145. *See* Headquarters, Department of the Army, FM 3-07 (FM 100-20), Stability Operations and Support Operations 1-1 (2003), *available at* http://usacac.army.mil/cac2/cgsc/carl/docrepository/fm3_07.pdf.

146. *See* DEPARTMENT OF PEACEKEEPING OPERATIONS, UNITED NATIONS PEACEKEEPING OPERATIONS: PRINCIPLES AND GUIDELINES 17 (2008), *available at* http://pbpu.unlb.org/pbps/library/capstone_doctrine_eNg.pdf (noting where the spectrum of peace and security activities is identified as conflict prevention, peacemaking, peacekeeping, peace enforcement and peace building).

147. *Id.*

block war,"[148] "revolutionary warfare,"[149] "irregular warfare,"[150] "war amongst the people,"[151] "mosaic war"[152] and "hybrid warfare."[153] One of the strengths of the legal approach, although also a potential weakness in terms of addressing new technology, has been its more consistent use of terminology. State legal advisors would likely have to present a convincing argument that terminology has to be changed. In this regard, they may be assisted if non-lawyers pause to think of the operational flexibility at the strategic level that the use of less warlike terms can offer.

IV. THE ROAD AHEAD

It is evident the cyber domain presents significant new challenges for interpreters of the *jus ad bellum*. A key issue to be addressed is the willingness of the international legal community to accept change to long-standing interpretations of the use of force under that body of law. For those lawyers who work for government, human rights advocates and academics, serious questions need to be asked—and answered—as to whether there is a need to create a whole new terminology and new principles regarding the use of cyber. This will present a daunting challenge for some parts of the international legal community who, even now, more than a decade after 9/11, either do not recognize[154] or only give grudging acceptance to the Security Council's determination that the right of self-defense under Article 51 can

148. *See* Charles C. Krulak, *The Strategic Corporal: Leadership in the Three Block War*, MARINES MAGAZINE, Jan. 1999, at 3, *available at* http://www.au.af.mil/au/awc/awcgate/usmc/strategic_corporal.htm.

149. *See* Bernard B. Fall, *The Theory and Practice of Insurgency and Counterinsurgency,* NAVAL WAR COLLEGE REVIEW, Winter 1998, at 46, 47.

150. *See* Kenneth C. Coons Jr. & Glenn M. Harned, *Irregular Warfare Is Warfare*, 52 JOINT FORCES QUARTERLY, Jan. 2009, at 97.

151. *See* GENERAL SIR RUPERT SMITH, THE UTILITY OF FORCE: THE ART OF WAR IN THE MODERN WORLD 3–4 (2007).

152. *See* Headquarters, Department of the Army & Headquarters, Marine Corps Combat Development Command, FM3-24/MCWP 3-33.5, Counterinsurgency ¶ 1–37 (2006).

153. DAVID KILCULLEN, THE ACCIDENTAL GUERRILLA: FIGHTING SMALL WARS IN THE MIDST OF A BIG ONE 4 (2009).

154. Randelzhofer, *supra* note 81, at 802 ("Acts of terrorism committed by private groups or organizations as such are not armed attacks in the meaning of Art. 51 of the UN Charter. But if large scale acts of terrorism of private groups are attributable to a State, they are an armed attack in the sense of Art. 51.").

be exercised against non-State actors who are not associated with a State.[155] As an initial foray into assessing cyber warfare in this context, the *Tallinn Manual* does not indicate that the necessary consensus will be easily reached on such a foundational issue. After reviewing what it describes as a controversial topic, it states "[s]uch State practice *appears* to signal a *willingness* of States to apply the right of self-defense to attacks conducted by non-State actors."[156] There is a very real danger that advances in technology are outstripping the pace of the legal dialogue.

It can only be hoped that more success is attained in clarifying the law surrounding the cyber domain than appears to have been the case with direct participation in hostilities. More than a decade after targeted killings attracted the attention of the international legal community, there still appears to be a lack of consensus on who qualifies as a lawful target. This is the case with regard to the question of whether members of organized armed groups can be targeted by virtue of their membership and, if so, how such membership is determined.[157] It was also noted in 2012 that "there is a range of views among the United States and its partners on the precise 'test' that should be applied to determine membership."[158] This is an area where the responsibility rests primarily with States, however, the State approach to defining that term still appears to be shrouded in a fog of ambiguity.

---

155. GRAY, *supra* note 82, at 198 (noting the reaction by states to the 9/11 attacks "may be seen as raising the question whether there has been a significant change in the law"). *But see* MOIR, *supra* note 129, at 51 ("[I]t would be extremely difficult to insist that the events of 11 September 2001 did not, and—in international law—*could not*, amount to an armed attack on the United States.") (emphasis added).

156. TALLINN MANUAL, *supra* note 4, rule 13, ¶ 16 (emphasis added).

157. Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions,

Study on Targeted Killings ¶ 65, Human Rights Council, U.N. Doc. A/HRC/14/24/Add.6 (May 28, 2010) (by Philip Alston),(2010), *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf ("In its general approach to DPH, the ICRC is correct to focus on function (the kind of act) rather than status (combatant vs. unprivileged belligerent) [of organized armed groups], but the creation of CCF [continuous combat function] category is, *de facto*, a status determination that is questionable given the specific treaty language that limits direct participation to 'for such time' as opposed to 'all the time.'").

158. Stephen Pomper*, Toward a Limited Consensus on the Loss of Civilian Immunity in Non-International Armed Conflict: Making Progress through Practice*, 88 NON-INTERNATIONAL ARMED CONFLICT IN THE TWENTY-FIRST CENTURY 181, 188–89 (Kenneth Watkin & Andrew J. Norris eds., 2012) (Vol. 88, U.S. Naval War College International Law Studies).

The fact that DPH is also an important issue for cyber warfare compounds the challenge facing those seeking to provide legal certainty to persons tasked with the responsible application of cyber force. Ambiguity as to how the law applies to cyber warfare has a positive aspect in that it provides operational space as a legal and policy consensus is being developed, while still acknowledging the requirement to operate within a legal envelope. However, the lack of certainty also potentially undermines the establishment of clear accountability "red lines." It can also have an adverse impact on the ability to control the actions of States, which, of course, is the very reason that the modern *jus ad bellum* and *jus in bello* were developed during the twentieth century.

If all of this is a challenge for government lawyers it may a greater one for those working for human rights advocacy groups. Certainly, there are options for human rights advocates to become cyber literate through access to academia and by hiring retired experts. They will also have to undergo a paradigm shift in their thinking, including expanding their horizons beyond the laws in war to the laws governing the recourse to war. Perhaps one of the most interesting aspects of cyber is that it has breathed life into the *jus ad bellum* discipline, which had fallen somewhat into the background of legal discussion given the predominance of non-international armed conflict in the post-Cold War era.[159]

States are testing the boundaries, not only of the technical applications of cyber, but also societal tolerance for its use or abuse. This presents a challenge for technical, operational and legal personnel interested in regulating its use. The information superhighway is becoming increasingly crowded with participants who are being forced to slow down, yield or perhaps even stop some activities. The intervention of lawyers will not always be seen as a positive development.[160] While cyber warfare developers and operators are being required to expose their inventions and capabilities, lawyers are finding themselves having to use nearly seventy-year-old law developed for different circumstances to deal with new technology. For those lawyers both inside and outside of government whose comfort zone

159. JACK S. LEVY & WILLIAM R. THOMPSON, CAUSES OF WAR 12 (2010) ("[T]here has been a shift in the nature of warfare over time—away from the great powers, away from Europe, and, increasingly, away from state-to-state conflict and toward civil war, insurgency, and other forms of intrastate and trans-state warfare.").

160. *See* Stewart Baker, *Denial of Service*, FOREIGN POLICY (Sept. 20, 2011), *available at* http://www.foreignpolicy.com/articles/2011/09/30/denial_of_service.

is "old rules" and "old conflicts," this will be a challenging time as they grapple with new technology and new warfare.

For lawyers embarked on this path to deal with the mankind's latest technological advancement, there is some hope that can be taken from history regarding their ultimate success in establishing a legal framework to govern its operations. Take an example from the *jus in bello* context, such as aerial warfare, where the law of armed conflict has been applied to new technology, in this case operating in "the third dimension."[161] The introduction of air warfare during the twentieth century presented a significant and daunting challenge to the legal community in its efforts to regulate its application during armed conflict. As was evident in the post-World War I debate over airpower, reaching consensus on regulation was difficult, as there were two "opposite tendencies . . . the ideology of extreme pacifists, well intentioned, good but utterly utopian and the thinking of hard and shrewd people . . . who wanted to keep their hands free as to the conduct of the next war."[162] Not only were initial efforts at regulating airpower through the development of the 1923 Hague Rules of Aerial Warfare largely unsuccessful,[163] one view in 1950 was that the use of airpower during World War II had reduced the principle of distinction to a hollow phrase: "in the matter of aerial bombardment there is no rule firmly grounded in the past on which we can place reliance—for aerial bombardment is a new weapon which raises new problems."[164]

It took the concern over wide-scale bombing in World War II, as well as the concerted attention of the human rights community in the 1960s and 1970s, for convention based legal rules for precautions governing targeting to be developed in Additional Protocol I.[165] These rules are now accepted

161. CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 4, at 121.

162. Kunz, *supra* note 142, at 39. *See also* DOCUMENTS ON THE LAWS OF WAR 140 (Adam Roberts & Richard Guelff eds., 2005) (explaining that "heightened awareness of the military potential of aircraft was a serious obstacle to reaching agreement").

163. DOCUMENTS ON THE LAWS OF WAR, *supra* note 162, at 139 ("The 1923 Hague Draft Rules were never adopted in legally binding form, but at the time they were regarded as an authoritative attempt to clarify and formulate rules of air warfare, and largely corresponded to customary rules and general principles underlying the laws of war on land and at sea.").

164. Hersh Lauterpacht, *The Problem of the Revision of the Law of War*, 29 BRITISH YEARBOOK OF INTERNATIONAL LAW 360, 364–66 (1952).

165. For an outline of the role in human rights non-governmental organizations in forcing the United Nations to take up the issue of the amendment of international humanitarian law, which led to Additional Protocol I and Additional Protocol II, see KEITH SUTER, AN INTERNATIONAL LAW OF GUERRILLA WARFARE 20–35 (1984).

as customary international law.[166] Renewed interest in aerial warfare has resulted in the development of the 2009 *Manual on International Law Applicable to Air and Missile Warfare*.[167] By the end of the first decade of the twenty-first century, the United States, as the preeminent world military power, is committed to these legal precautions. This is evidenced by the statements of senior government officials regarding targeting during counterterrorism operations.[168]

Given the pace of technological advances, however, it is clear that the regulation of the cyber domain in either a *jus ad bellum* or *jus in bello* context cannot be allowed to follow the same difficult and tortoise like path to regulation of air warfare as occurred last century. There are signs that this will occur, although it is always necessary to remember that verbal statements to follow fundamental humanitarian law principles regarding aerial warfare were also expressed immediately prior to World War II.[169] There has al-

---

166. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW STUDY 51 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005).

167. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE (2009), *available at* http://www.ihlresearch.org/amw/manual/.

168. Harold Hongju Koh, Legal Advisor, Department of State, Address at the Annual Meeting of the American Society of International Law (Mar. 25, 2010), *available at* http://www.state.gov/s/l/releases/remarks/139119.htm ("In particular, this Administration has carefully reviewed the rules governing targeting operations to ensure that these operations are conducted consistently with law of war principles. . . ."); Jeh Charles Johnson, General Counsel, Department of Defense, Speech at Yale Law School (Feb. 22, 2012), *available at* http://www.cfr.org/national-security-and-defense/jeh-johnsons-speech-national-security-law-lawyers-lawyering-obama-administration/p27448 ("[T]here is no prohibition under the law of war on the use of technologically advanced weapons systems in armed conflict, so long as they are employed in conformity with the law of war."). Attorney General Eric Holder has also stated, with regard to the use of lethal force:

> Of course, any such use of lethal force by the United States will comply with the four fundamental law of war principles governing the use of force. The principle of necessity requires that the target have definite military value. The principle of distinction requires that only lawful targets – such as combatants, civilians directly participating in hostilities, and military objectives – may be targeted intentionally. Under the principle of proportionality, the anticipated collateral damage must not be excessive in relation to the anticipated military advantage. Finally, the principle of humanity requires us to use weapons that will not inflict unnecessary suffering.

Eric Holder, U.S. Attorney General, Address at Northwestern University School of Law (Mar. 5, 2012), *available at* http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1203051.html.

169. DOCUMENTS ON THE LAWS OF WAR, *supra* note 162, at 140 (outlining the statement by British Prime Minister Neville Chamberlain on June 21, 1938 on three fundamen-

ready been a commitment by the United States regarding the application of not only the *jus ad bellum*, but also the law of armed conflict to cyber operations conducted during armed conflict.[170] What is not known at this stage is what adherence to broad legal principles means in practical terms during cyber operations or how it will be interpreted in responding to cyber attacks. It is here that the operationalization of international law in the cyber domain by all States will fully demonstrate that commitment. Until the technical, policy and legal communities merge on the cyber highway and "rules of the road" are not only agreed to, but acted upon, it may be the principle of reciprocity that keeps cyber within the lanes as the law catches up to the latest means of warfare that the human mind has developed.[171]

Finally, in assessing the impact of international law on the cyber domain, what cannot be forgotten is that the threshold for armed attack provides, in practical terms, the setting of a threshold for war. As has been noted by David Rodin, wars are hugely complex events, impacted by unpredictable eventualities and which "have a peculiar internal dynamic of their own which often subverts the original objectives and commitments of those who initiate them."[172] Caution will have to be applied in considering the threshold for cyber-based armed attacks given the considerable humanitarian, financial and reputational costs armed conflict inevitably entails.

---

tal principles applicable to aerial warfare: no direct attacks against the civilian population, only target legitimate military objectives and take care to "avoid bombardment of a civilian population in the neighbourhood").

170. *Koh Remarks*, *supra* note 100; *See also* Waxman, *supra* note 44, at 433 n.57 (outlining the testimony of Lieutenant-General Keith Alexander who asserts that returning fire in cyberspace would be lawful "as long as it complied with law of war principles").

171. Eric Schmitt & Thom Shanker, *U.S. Debated Cyberwarfare in Attack Plan on Libya*, NEW YORK TIMES (Oct. 17, 2011), http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html (discussing potential cyber operations to impair Libyan air defenses in March 2011 and explaining that "administration officials and even some military officers balked, fearing that it might set a precedent for other nations, in particular Russia or China, to carry out such offensives of their own").

172. DAVID RODIN, WAR & SELF-DEFENSE 11 (2002).