INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1901
U.S. NAVAL WAR COLLEGE

Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?

John F. Murphy

89 INT'L L. STUD. 309 (2013)

Volume 89 2013

Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?

John F. Murphy[*]

I. INTRODUCTION

As the concluding speaker at the conference on "Cyber War and International Law," co-sponsored by the Naval War College and the United States Cyber Command, Yoram Dinstein, Professor Emeritus at Tel Aviv University, professed some disappointment that there had not been a more extensive and sharper focus at the conference on "war."[1] But perhaps the limited amount of discussion of cyber "war" at the conference was a result of the reality that the international law issues arising from the possibility of war or armed conflict through cyber means have not been the primary concern of States and scholars faced with the challenges of the cyber threat. Rather, at least in the United Nations General Assembly and other international fora, such as the International Telecommunications Union (ITU), the threat posed by such adversaries of the United States as the Russian Federation and China seems to be an effort to adopt a global treaty

* Professor of Law, Villanova School of Law. I want to acknowledge the excellent research assistance of Lori Strickler, Reference Librarian, Villanova University School of Law; and Daria Hafner and Karrie Gurbacki, both second-year students at Villanova University School of Law.

1. See Yoram Dinstein, *Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference*, 89 INTERNATIONAL LAW STUDIES 276 (2013).

that would arguably allow increased regulation by the United Nations—and perhaps the ITU—that would endanger the free flow of information on the Internet and such basic values as privacy and freedom of speech. To be sure, a hostile takeover of the Internet could have serious implications for U.S. vulnerability to cyber attack and thereby amount to a serious threat to its national security, but this is a far cry from possible revisions of the *jus ad bellum* and *jus in bello* associated with cyber war, which is to the disadvantage of the United States.

The title of this article poses the question whether, in the context of cyber war and other related forms of cyber attack, the international legal process itself may pose a threat to vital U.S. interests. Certainly, as we shall see below, a successful effort by the Russian Federation and China to conclude a widely adopted global treaty authorizing the United Nations or the ITU to regulate the Internet would constitute such a threat. Moreover, in *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,*[2] the International Court of Justice (ICJ) in an advisory opinion stated that "Article 51 of the Charter thus recognizes the existence of an inherent right of self-defence in the case of armed attack by one State against another State. However, Israel does not claim that the attacks against it are imputable to a foreign State."[3]

Similarly, in *Armed Activities on the Territory of the Congo,*[4] the ICJ rejected Uganda's claim that it had engaged in lawful military activity in Congo's territory to protect itself against insurgents who had organized themselves there to commit armed attacks against Uganda's territory. If the Court's viewpoint is correct, this would have very serious implications for the right of self-defense against cyber attacks because many, perhaps most, of such attacks are committed by non-State actors. The problem is compounded by the often present difficulty in determining who or what actually engaged in the attack (the problem of attribution). Fortunately, for reasons considered later in this article, the Court's viewpoint, which has been subject to withering criticism, is almost surely not correct. But the primary point to take away here is that one of the most important actors in the international legal process, the ICJ, has adopted a legal position that greatly threatens vital

2. Legal Consequences of the Construction of Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 (July 9).

3. *Id.* ¶ 139.

4. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168 (Dec. 19).

U.S. interests, as well as those of many other States in the international community.[5]

Speaking of vital U.S. interests, there have been recent developments in cyber space that raise the issue of U.S. interests in sharp relief. These developments involve four (apparently) State-sponsored computer viruses with the nicknames Stuxnet, Duqu, Flame and Gauss. The goals behind the development of these viruses vary. Stuxnet, for example, first became public knowledge in July 2010. It has been described as "far more complex than run-of-the mill hacker tools" and as

> a self-replicating worm that targeted programmable logic controllers (PLCs), the simple computers used to perform automated tasks in many industrial processes. PLCs are part of industrial control systems, most commonly referred to as Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are critical to the modern industrial world, controlling such things as water plants, auto manufacturing, and electrical power grids.[6]

According to the same commentator,

> [t]he Stuxnet code showed up on computer systems around the world, where it parked on hard drives, remaining inert if it did not find what it was seeking. The numbers indicate it was aimed at Iran; nearly 60 percent of reported Stuxnet infections occurred on systems in Iran. In fact, at least one system Stuxnet was programmed to target [were] controlled centrifuges critical to the production of nuclear material. It appears that Iran's uranium enrichment facility at Natanz was the specific target."[7]

In other words, the purpose behind Stuxnet was to undermine the Iranian nuclear program which, it is believed, is designed to produce a nuclear bomb. According to reports,[8] a series of Stuxnet attacks temporarily took

---

5. For analysis and criticism of other decisions and advisory opinions of the ICJ that arguably undermine the vital interests of States, see JOHN F. MURPHY, THE EVOLVING DIMENSIONS OF INTERNATIONAL LAW: HARD CHOICES FOR THE WORLD COMMUNITY 65–75 (2010).

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

7. *Id.*

8. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES, June 1, 2012, at A1, *available at* http://www.nytimes.com/2012/06/01/

out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium. As to who was behind these Stuxnet attacks, although the evidence is not entirely conclusive, there are numerous indications it was the United States and Israel.[9]

In contrast to Stuxnet, it appears the primary purpose behind the Doqu, Flame and Gauss viruses is cyber espionage. For example, a *Washington Post* article reported that the United States and Israel developed the Flame virus to gather intelligence "in preparation for cyber-sabotage aimed at slowing Iran's ability to develop a nuclear weapon."[10]

There is substantial support for the proposition that international law does not regulate espionage, although as is shown below, this proposition is controversial. There is also an issue whether, in any event, the same can be said of cyber espionage.

This article begins with a discussion of the legality (or not) of Stuxnet and the other recently developed viruses under current international law, specifically the *jus ad bellum* and the *jus in bello,* as well as an analysis of whether traditional forms of espionage or the emerging practice of cyber espionage are covered by current international law. It then turns to an examination of recent efforts by Russia, China and others to develop an international law treaty for regulating the Internet, and efforts by Russia in particular to conclude a treaty on cyber war, and the extent to which these efforts may represent a use of the international legal process that threatens U.S. vital interests. Next the article explores some of the legal implications of the claim that the United States has conflated the terms "use of force" in Article 2(4) and "armed attack" in Article 51 of the UN Charter in such a way as to support an overly expansive interpretation of the right of self-defense under Article 51. Lastly, the article considers some of the challenges that the use of cyber warfare by terrorists may pose to international law and policy.

---

world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r= 0.

9. *Id.*

10. *See* Ellen Nakashima, Greg Miller & Julie Tate, *U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*, WASHINGTON POST (June 19, 2012), http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

II. THE COMPATIBILITY OF STUXNET WITH CURRENT INTERNATIONAL LAW AND THE APPLICABILITY, IF ANY, OF INTERNATIONAL LAW TO TRADITIONAL ESPIONAGE OR CYBER ESPIONAGE

A. Stuxnet

In various writings and various forums, Michael Schmitt has extensively explored the *jus ad bellum* aspects of cyber operations.[11] He has also extensively explored the *jus in bello* dimensions of cyber operations.[12] With respect to the *jus ad bellum* dimension of Stuxnet, the key issue is whether the Stuxnet virus directed against Iran's centrifuges constitutes a "use of force" prohibited by Article 2(4) of the UN Charter. Schmitt poses the applicable test as follows:

> That the term "use of force" encompasses resort to armed force by a state, especially force levied by the military is self-evident. Armed force thus includes kinetic force—dropping bombs, firing artillery, and so forth. It would be no less absurd to suggest that cyber operations that generate consequences analogous to those caused by kinetic force lie beyond the prohibition's reach, than to exclude other destructive non-kinetic actions, such as biological or radiological warfare. Accordingly, cyber operations that directly result (or are likely to result) in physical harm to individuals or tangible objects equate to armed force, and are therefore uses of force. For instance, those targeting an air traffic control system or a water treatment facility clearly endanger individuals and property.[13]

To my knowledge, Stuxnet did not threaten or cause physical harm to individuals, but as noted previously, it did cause physical harm to 1,000 centrifuges critical to the production of nuclear material by Iran. This would

---

11. See, e.g., Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, 56 VILLANOVA LAW REVIEW 559 (2011). Another major article, which also explores the *jus in bello* dimensions of cyber operations, is 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).

12. *See* Michael N. Schmitt, *Cyber Operations and the* Jus in Bello*: Key Issues*, *in* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 89 (Raul A. "Pete" Pedrozo and Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies). *See also* Michael N. Schmitt, *Classification of Cyber Conflict*, 89 INTERNATIONAL LAW STUDIES 233 (2013).

13. Schmitt, *Cyber Operations and* the Jus ad Bellum *Revisited*, *supra* note 11, at 573.

seem to qualify as the kind of consequences to tangible property analogous to those caused by kinetic force suggested by Schmitt.

To be sure, Article 2(4)'s prohibition of the use of force applies by its terms only to "Members" of the United Nations.[14] This raises the issue of attribution, i.e., unless the use of the Stuxnet virus can be attributed to a State there is no violation of Article 2(4). As indicated earlier in this article, however, there is considerable evidence that the United States and Israel were behind the Stuxnet attacks.[15] For example, writing in the *New York Times* on June 1, 2010,[16] David Sanger reports that during his first months in office, President Obama "secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program."[17] The expanded first U.S. sustained use of cyber weapons that Sanger refers to had begun in the George W. Bush administration and was code named Olympic Games. It remained secret until the summer of 2010 when a programing error allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the virus gave it the nickname Stuxnet. According to Sanger, even after Stuxnet became public, President Obama decided to continue using it and after a few weeks of a series of attacks the result was that 1,000 of the 5,000 centrifuges Iran had spinning to purify uranium were temporarily taken out of commission.[18]

There is further evidence that the United States and Israel were behind the Stuxnet attacks.[19] First, the use of zero-day hacks (a zero-day hack exposes vulnerability in a piece of software that was previously unknown to the developer) demonstrates that this was likely the work of multiple programmers with a substantial budget. Indeed, some analysts have estimated that "it could have taken five to ten programmers upwards of six months

14. Article 2(4) of the UN Charter provides: "All Members shall refrain in their international relations from the use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

15. *See supra* notes 8 and 9 and accompanying text.

16. *See* Sanger, *supra* note 8.

17. *Id.*

18. *Id.*

19. *See* Jeremy Richard, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INTERNATIONAL LAW JOURNAL 842, 854 (2012).

to create Stuxnet."[20] Moreover, Stuxnet is a "highly specialized piece of malware" and "the narrow range of circumstances in which Stuxnet would deploy its payload makes it unlikely that Stuxnet had another purpose besides destroying nuclear centrifuges."[21] Additionally, the Israeli government's responses to news of the virus were highly suspicious. When Israeli officials were asked about their involvement in Stuxnet they "broke into wide smiles."[22] Also, a video played at the retirement party of former Israeli Defense Force Chief of General Staff Lieutenant General Gabi Ashkenazi featured references to Stuxnet as one of the general's operational successes, and, for its part, the United States has refused to deny involvement in Stuxnet.[23]

Assuming arguendo that Stuxnet constitutes a use of force in violation of Article 2(4) of the UN Charter,[24] the issue then arises whether it also constitutes an armed attack that would give Iran a right to exercise self-defense under Article 51 of the UN Charter.[25] At the time of this writing, the U.S. government has not publicly articulated a general position on cyber attacks and Articles 2(4) and 51.[26] There is some evidence that the United States has conflated the terms "use of force" under Article 2(4) and "armed attack" under Article 51, with the result that a cyber attack that constituted a use of force would also qualify as an armed attack, giving rise to a right of self-defense on the part of the State suffering the attack to engage in a military use of armed force.[27] But Michael Schmitt, along with

---

20. *Id.*

21. *Id.*

22. *Id.* at 856.

23. *Id.*

24. It is worth noting that in an email of August 14, 2012 to me, Michael Schmitt stated that in his opinion Stuxnet was a use of force under Article 2(4) (email on file with author).

25. Article 51 of the UN Charter reads as follows:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

26. *See* Matthew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 431 (2011).

27. For discussion, see *id.* at 431–37.

other commentators, rejects the idea that there is no difference between "a use of force" under Article 2(4) and an "armed attack" under Article 51. In Schmitt's view:

> The key text in Article 51, and the foundational concept of the customary law right of self-defense, is "armed attack." But for an armed attack, States enjoy no right to respond forcefully to a cyber operation directed against them, even if that operation amounts to an unlawful use of force. This dichotomy was intentional, for it comports with the general presumption permeating the Charter scheme against the use of force, especially unilateral action. In the *Nicaragua* case, the ICJ acknowledged the existence of this gap between the notions of use of force and armed attack when it recognized that there are "measures which do not constitute an armed attack but may nevertheless involve a use of force" and distinguished "the most grave forms of the use of force from other less grave forms." Recall that the court specifically excluded the supply of weapons and logistical support to rebels from the ambit of armed attack, but noted that such actions might constitute uses of force. Simply put, all armed attacks are uses of force, but not all uses of force qualify as armed attacks.[28]

Not all uses of force qualify as armed attacks, but some do, and the issue is whether Stuxnet qualifies as one of those that do. Schmitt has noted, correctly in my view, that "Article 51 restricts a state's right of self-defense to situations involving *armed* attack, a narrower category of act than Article 2(4)'s use of force."[29] Schmitt goes on to add: "Thus, faced with CNA [computer network attack] that does not occur in conjunction with, or as a prelude to, conventional military force, a state may only respond with force in self-defense if the CNA constituted armed force . . . intended to directly cause physical destruction or injury."[30] Under this standard, there would seem to be little doubt that Stuxnet qualified as an armed attack under Article 51. It should be noted, however, that Yoram Dinstein has argued that to qualify as an "armed attack" a cyber attack must produce "violent consequences."[31] In response to this argument, Matthew Waxman has suggested that

---

28. *See* Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, *supra* note 11, at 587.

29. *See* Schmitt, *Computer Network Attack and the Use of Force in International Law*, *supra* note 11, at 928.

30. *Id.* at 929.

31. *See* Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99, 103 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (Vol. 76, U.S. Naval War College International Law Studies) ("The

> [a] significant problem with this view is that in a world of heavy economic, political, military, and social dependence on information systems, the 'nonviolent' harms of cyber-attacks could easily dwarf the 'violent' ones. Consider, for example, a take-down of banking systems, causing cascades of financial panic, or the disabling of a power grid system for an extended period of time, causing massive economic disruption and public health emergencies.[32]

In his statement quoted above, Schmitt notes that the ICJ in the *Nicaragua* case supports the proposition that there is a gap between the notions of use of force and armed attack. It is important to note, however, that the U.S. government has emphatically rejected the Court's analysis in *Nicaragua*, as well as a similar analysis in the later ICJ decision in the *Oil Platforms* case.[33] Specifically, as to the *Nicaragua* decision, Abraham D. Sofaer, then-Legal Adviser of the U.S. Department of State, in a luncheon address jointly sponsored by the American Society of International Law and the Section of International Law and Practice,[34] sharply criticized the ICJ's comments on the right of self-defense, especially its narrow definition of the scope of the term "armed attack" to exclude "assistance to rebels in the form of the provision of weapons or logistical or other support."[35] In Sofaer's view, "[t]his ruling was without support in customary international law, or the practice of nations, which could not rationally be read to deprive a state of the right to defend itself against so serious a form of aggression."[36] Sofaer added that

> the ICJ's ruling concerning the use of force creates artificial distinctions and mechanical rules that are fundamentally inconsistent with the principled but flexible approach followed by the United States since the Charter's adoption. Its restrictive approach in defining "armed attack" could deprive states of the right of self-defense against the most common and dangerous forms of aggression in the world today.[37]

---

crux of the matter is not the medium at hand . . . but the violent consequences of action taken.").

32. See Waxman, *supra* note 26, at 436.

33. *See* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161 (Nov. 6).

34. *See* Abraham D. Sofaer, *International Law and the Use of Force*, 82 AMERICAN SOCIETY OF INTERNATIONAL LAW PROCEEDINGS 420 (1988).

35. *Id.* at 425.

36. *Id.*

37. *Id.* at 426.

Writing in the *Yale Journal of International Law* in 2004,[38] William H. Taft, IV, then-Legal Adviser of the U.S. Department of State, was perhaps even more scathing in his criticism of the ICJ's comments on self-defense under international law in the *Oil Platforms* case than was Sofaer with respect to the Court's decision in *Nicaragua*. In *Oil Platforms*, Iran claimed that the United States had violated the "freedom of commerce" provision in the 1955 Treaty of Amity, Economic Relations and Consular Rights between the two countries by taking military action against Iranian offshore oil platforms in 1987 and 1988. Interestingly, the ICJ rejected Iran's claim, finding that the U.S. actions against the oil platforms did not disrupt commerce between the territories of Iran and the United States. In other words, the United States won the case. Nonetheless, the Court proceeded to devote "a substantial portion of its opinion to a consideration of whether the U.S. actions against the oil platforms qualified as self-defense under international law. The Court's statements concerning this issue were unnecessary to resolve the case and thus, in our domestic legal system, would be considered non-binding *dicta*."[39]

Parenthetically, I would suggest that Taft's characterization of the ICJ's statements as non-binding *dicta* was overly restrained. I would characterize the Court's discussion of whether the U.S. action against the oil platforms qualified as self-defense under international law as an outrageous abuse of the judicial process. Having decided that Iran had no claim under the Treaty of Amity with the United States, the Court had no legitimate reason to express its view on another argument the United States had made in response to Iran's claim. The Court was, after all, rendering a decision in a contentious case, not handing down an advisory opinion.[40]

Be that as it may, Taft argued that the Court's statements in the *Oil Platform* case concerning self-defense might be read as suggesting a number of limitations on the right of self-defense, namely:

- that an attack involving the use of deadly force by a State's regular armed forces on civilian or military targets is not an "armed attack"

38. William H. Taft, IV, *Self-Defense and the Oil Platforms Decision*, 29 YALE JOURNAL OF INTERNATIONAL LAW 295, 295 (2004) (emphasis in original).

39. *Id.*

40. In his article, Taft did note that five of the judges on the Court had expressly raised concerns about the majority's decision to address the issue of self-defense. *See id.* at 298. The five judges, all of whom wrote separate opinions, were Buergenthal, Higgins, Parra-Aranguren, Kooijmans and Owada.

> triggering the right of self-defense, unless the attack reaches some unspecified level of gravity;
> - that an attack must have been carried out with the intention of harming a specific State before that State can respond in self-defense; that self-defense may be directed only against targets of the attacking State that have been the subject of specific prior complaints by the defending State; and
> - that measures taken in self-defense must be proportional to the particular attack immediately preceding the defensive measures rather than proportional to the overall threat being addressed.[41]

Taft next stated categorically that "international law and practice do not support these limitations on the right of self-defense" and added, perhaps contrary to the fact, that "[t]he United States presumes that the Court did not intend to suggest these limitations."[42]

Interestingly, under either the Schmitt approach to armed attack,[43] the U.S. practice of conflating Article 2(4) and Article 51 or the ICJ's narrower definition of the scope of self-defense, there is a strong argument to be made that Stuxnet constituted both a use of force under Article 2(4) and an armed attack under Article 51. If so, it may seem odd that Iran's reaction to this cyber attack was so restrained, almost to the point of not acknowledging its existence. Indeed, although Iranian officials initially stated that a delay in its Bushehr nuclear power plant being operational was based on "technical reasons," it did not complain of it being the result of a cyber attack.[44] Later, Iran's President, Mahmoud Ahmadinejad, reported that malicious software had damaged the centrifuge facilities, but did not suggest that Iran had been the victim of a State-sponsored cyber attack, much less that it had been the victim of an armed attack and therefore had the right to respond with armed force in the exercise of its right of self-defense under Article 51.[45] It is unclear why Iran's reaction to the Stuxnet attack was so restrained,[46] but one result of this restraint is that there has been rela-

---

41. *Id.* at 299.

42. *Id.*

43. In his email to me of August 14, 2012, Michael Schmitt stated that it was his opinion that Stuxnet was both a use of force under Article 2(4) of the UN Charter and an armed attack under Article 51. *See supra* note 24.

44. *See* Brown, *supra* note 6.

45. *Id.*

46. In his article Gary Brown speculates about a variety of possible reasons for Iran's restraint. *See id.*

tively little reaction to Stuxnet in the world community and only a smattering of coverage in the media or legal literature.

B. International Law and Traditional Espionage

Several times during the "Cyber War and International Law" conference categorical comments were made that espionage is not prohibited by international law.[47] If one is considering traditional espionage, it is important to distinguish between espionage in war or armed conflict and peacetime espionage. Most scholarly writing on the relationship between espionage and international law concerns the law of war or armed conflict.[48] John Radsen has suggested:

> The rules of espionage in times of war, whether based on the Hague Regulations of 1907, the Geneva Conventions, the Protocol Additional to the Geneva Conventions, or other sources, are straightforward. A "scout," someone who stays in military uniform or sufficiently designates himself as a combatant, risks being caught behind enemy lines. If caught, this person should be dealt with as a prisoner of war because there is nothing treacherous or deceitful about his scouting or reconnaissance mission. But a spy, someone who does not wear a military uniform or a clear military designation, is not entitled to protection as a prisoner of war. His deceit can lead to severe punishment from the captors. Despite the potentially harsh penalties, the trial itself for the charge of espionage should follow standard procedures. Note, by the way, that if the spy returns to his military organization after his mission and is then captured in battle wearing a Soldier's uniform or designation, he cannot be punished for his prior act of spying. A spy therefore has a strong incentive to succeed in his spying mission and to return quickly to his military organization.[49]

The situation concerning espionage and international law outside of the law of war is much less straightforward. Indeed, Radsen quotes with approval as having contemporary relevance, a 1962 statement by Richard Falk: "[t]raditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether

47. *See, e.g.*, Dinstein, *supra* note 1, at 284.

48. *See* John Radsen, *The Unresolved Equation of Espionage and International Law*, 28 MICHIGAN JOURNAL OF INTERNATIONAL LAW 595, 601 (2007).

49. *Id.* at 602.

or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture."[50]

Radsen goes on to report that the limited literature available on peacetime espionage can be divided into three groups:

> One group suggests peacetime espionage is legal (or not illegal) under international law. Another group suggests peacetime espionage is illegal under international law. A third group, straddled between the other two, maintains that peacetime espionage is neither legal nor illegal—perhaps, as Nietzsche would say, that it is beyond good and evil. In any event, the uncertainty in the literature supports my thesis that espionage is beyond international consensus.[51]

Of the three groups discussed by Radsen, the one that seems most convincing to me is the third: the group holding that espionage is neither legal nor illegal. In his discussion of the literature in the third group, Radsen quotes a writing by two former CIA officials, Daniel Silver, a former General Counsel, and Frederick Hitz, a former Inspector General.[52] In their writing, Silver and Hitz state that "[t]here is something almost oxymoronic about addressing the legality of espionage under international law."[53] Referring to the "ambiguous state of espionage under international law,"[54] they conclude that espionage is neither clearly condoned nor condemned under international law. Radsen adds by way of comment that:

> The rules and the ethics are situational. Countries are much less tolerant when espionage is committed against them than when they are committing it against friends and foes. Whether espionage is legal or illegal under international law, they are realistic about the fact that countries, for reasons of self-defense and for their own interests, are going to commit espionage in other countries. According to Silver and Hitz, that may explain why no treaties or conventions specifically prohibit espionage.[55]

---

50. *Id.* The cite to Falk is Richard Falk, *Foreword to* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, at v, v (Roland J. Stanger ed., 1962).

51. Radsen, *supra* note 48, at 602.

52. *Id.* at 606.

53. Daniel B. Silver (updated and revised by Frederick P. Hitz & J.E. Shreve Ariail), *Intelligence and Counterintelligence*, *in* NATIONAL SECURITY LAW 935, 965 (John Norton Moore & Robert F. Turner eds., 2d ed. 2005).

54. *Id.*

55. Radsen, *supra* note 48, at 606.

C. Cyber Espionage and International Law

Cyber espionage is a relatively new development that raises a basic question: Does cyber espionage differ from traditional espionage simply as a matter of degree, or is it an entirely new phenomenon that arguably poses new challenges for international law and practice? In addressing this issue, it is helpful to consider the workings of the new computer viruses with the nicknames Flame and Gauss.

The British Broadcasting Corporation first began reporting about the Flame virus in May 2012 after the Russian security firm Kaspersky Lab began investigating the matter.[56] The ITU had asked Kaspersky Lab to look into reports in April that computers belonging to the Iranian Oil Ministry and the Iranian National Oil Company had been hit with malware that was stealing and deleting information from their systems.

Flame is designed to monitor computer networks and send back intelligence to its creators.[57] It reportedly has the capacity to "activate computer microphones and cameras, log keyboard strokes, take screen shots, extract geolocation from images, and send and receive commands and data through Bluetooth wireless technology."[58] It also reportedly is more than twenty times larger than Stuxnet, and, most important, "whereas Stuxnet just had one purpose in life, Flame is a toolkit, so they can go after just about everything they can get their hands on."[59] Along the same lines, Kaspersky Lab's chief malware expert Vitaly Kamluk has reportedly described Flame as "basically an industrial vacuum cleaner for sensitive information."[60]

The virus appears to have a wide reach indeed, as more than six hundred specific targets were hit, ranging from individuals, businesses and academic institutions to government systems. Iran's National Computer Emergency Response Team posted a security alert stating that it believed Flame was responsible for "recent incidents of mass data loss" in the coun-

---

56. Reuven Cohen, *New Massive Cyber-Attack an "Industrial Vacuum Cleaner for Sensitive Information,"* FORBES (May 28, 2012), http://www.forbes.com/sites/reuvencohen/2012/05/28/new-massive-cyber-attack-an-industrial-vacuum-cleaner-for-sensitive-information/.

57. *See* Nakashima, Miller & Tate, *supra* note 10.

58. *Id.*

59. David Lee, *Flame: Massive Cyber-Attack Discovered, Researchers Say*, BBC NEWS (May 28, 2012), http://www.bbc.co.uk/news/technology-18238326.

60. *Id.*

try.[61] Among the countries affected by the virus are Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia and Egypt. Further instances of infected machines were detected in the United States, as well as in the United Kingdom and parts of Europe. Researchers, however, pointed out this did not necessarily mean these countries were targets, as "use of proxy servers can distort location data."[62]

Although the basic purposes behind Stuxnet and Flame appear to differ, the two viruses are similar in a number of ways, including the "names of mutually exclusive objects, the algorithm used to decrypt strings, and the similar approaches to file naming"; moreover, parts of the code are identical, especially the part responsible for the virus's distribution.[63] Alexander Gostev, chief security expert of Kaspersky Lab, described these similarities between the two viruses as "very strong evidence that Stuxnet/Duqu and Flame cyber-weapons are connected."[64]

A recent *Washington Post* article directly attributed Flame to the United States and Israel, stating that they developed the virus to gather intelligence "in preparation for cyber-sabotage aimed at slowing Iran's ability to develop a nuclear weapon."[65] Both American and Israel officials, however, have denied the *Washington Post*'s claim, and the evidence is conflicting.[66]

Kaspersky Lab recently discovered the fourth allegedly State-sponsored computer virus to surface in the Middle East in the past three years, apparently aimed at computers in Lebanon.[67] According to Kaspersky Lab, the virus appeared to have been written by the same programmers who created Flame and may be linked to Stuxnet. This latest virus, nicknamed Gauss after a name found on its code, has been detected on 2,500 computers, most of them in Lebanon. The firm said its purpose appeared to be to acquire

---

61. *Id.*

62. *Id.*

63. *See Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected,* KASPERSKY LAB (June 11, 2012), http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected.

64. *Id.*

65. *See* Nakashima, Miller & Tate, *supra* note 10.

66. *See* Sanger, *supra* note 8 (U.S. officials denying Flame was part of Olympic Games); Hayley Tsukayama, *Flame Cyberweapon Written Using Gamer Code, Report Says*, WASHINGTON POST (May 31, 2012), http://articles.washingtonpost.com/2012-05-31/business /35456034_1_stuxnet-flame-virus-skywiper%20 (Israel's denial of involvement with Flame).

67. *See* Nicole Perlroth, *Computer Virus Is Aimed at Banks in Lebanon, Security Firm Says*, NEW YORK TIMES, Aug. 10, 2012, at A4.

"logins for email and instant messaging accounts, social networks and, notably, accounts at certain banks—a function more typically found in malicious programs used by profit-seeking cybercriminals."[68]

Lebanese experts reportedly said that an American cyber espionage campaign directed at Lebanon's banking system was plausible, given U.S. concerns that the country's banks are being used as a financial conduit for the Syrian government and for Hezbollah, the Lebanese militant group and political party. Researchers at Kaspersky Lab stated they were confident that Gauss was the work of the same hands as Flame, because the viruses were written in the same language (known as C++) on the same platform and shared some code and features.[69]

At a minimum, it is clear that computer viruses such as Flame and Gauss constitute a method of espionage whose efficiency greatly exceeds that of traditional espionage. If Flame, for example, truly is "basically an industrial vacuum cleaner for sensitive information," it raises an unprecedented threat to the national security interests of targeted States. It has been argued that only Russia, China, Israel and the United States have the capability of engaging in such sophisticated espionage.[70] And there appears little doubt that the United States has an extraordinary capacity to engage in such espionage. Richard Clarke, however, who served three presidents as a counterterrorism czar, has argued that, although the United States has developed the capability to conduct an offensive cyber war, it has virtually no *defense* against the cyber attacks he says are targeting it now, and those that will be in the future.[71]

Clarke argues further that China in particular is engaged in cyber espionage that greatly threatens U.S. national security and goes so far as to claim that "[e]very major company in the United States has already been penetrated by China."[72] As an example, Clarke argues that the manufacturer of the F-35, the U.S. next generation fighter bomber, has been penetrated and

---

68. *Id.*

69. *Id.*

70. *See* Stephen Dockerty, *Virus Plunges Lebanon into Cyber War,* THE DAILY STAR (Aug. 11, 2012), http://www.dailystar.com.lb/News/Local-News/2012/Aug-11/184234-virus-plunges-lebanon-into-cyber-war.ashx#axzz2GqgfT6Pm.

71. This is the basic theme of RICHARD A. CLARKE & ROBERT KNAKE, CYBER WAR (2010). *See also* Ron Rosenbaum, *Richard Clarke on Who Was Behind the Stuxnet Attack*, SMITHSONIAN, Apr. 2012, at 12, *available at* http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html (in which the author interviews Clarke).

72. *Id.* at 17.

the F-35 details stolen. He also contends that our supply chain of chips, routers and hardware imported from China and other foreign suppliers may have been implanted with "logic bombs," trapdoors and "Trojan Horses," all ready to be activated on command. As a result, Clarke is reported as saying:

> My greatest fear is that, rather than having a cyber-Pearl Harbor event, we will instead have this death of a thousand cuts. Where we lose our competitiveness by having all of our research and development stolen by the Chinese and we never really see the single event that makes us do something about it.[73]

Clarke's concerns go way beyond the cost of lost intellectual property, and focus on the possible loss of military power. He envisions a confrontation, like the one in 1996 when President Clinton rushed two carrier battle groups to the Taiwan Strait to warn China against an invasion of Taiwan. This time, he suggests,

> we might be forced to give up playing such a role for fear that our carrier group defenses could be blinded and paralyzed by Chinese cyberintervention. (He cites a recent war game published in an influential military strategy journal called *Orbis* "How the U.S. Lost the Naval War of 2015").[74]

It is arguable that the use of cyber viruses with the efficiency of Flame or Gauss for espionage purposes constitutes a violation of current international law. As indicated previously,[75] Iran's National Computer Emergency Response team posted a security alert stating that it believed that Flame was responsible for recent incidents of "mass data loss" in the country. If one views data as a form of property, indeed a very important form of property in the modern world, a mass loss of data could constitute an armed attack. Also, if Clarke's allegation that China has penetrated by cyber means every major company in the United States, with the result that major military assets like advanced fighter jets and aircraft carriers have been compromised or even rendered dysfunctional is true, this raises the issue of the need for anticipatory self-defense against a great threat to U.S. national

73. *Id.*
74. *Id.*
75. *See* Lee, *supra* note 59 and accompanying text.

security—"perhaps the most controversial question in relation to the right of self-defence."[76]

To be sure, Christopher Greenwood, a judge on the ICJ, has stated that claims that cyber attacks should be considered armed attacks should be "treated with considerable caution."[77] Judge Greenwood suggests:

> The planting of a virus or the use of other computer techniques to undermine, for example, the computer systems regulating a State's financial system or immigration controls is difficult to see as an armed attack. Although the consequences of such conduct may be very serious, it seems closer to the concept of economic coercion. On the one hand, if such action were used to produce results similar to those which could otherwise be achieved only by the use of armed force, for example, causing aircraft to crash or dams to open and flood areas of a State's territory, then the argument that such action should be treated as a form of armed attack is more plausible.[78]

Judge Greenwood's words of "considerable caution" should be taken seriously. In his article, however, there is no discussion of the four advanced computer viruses, which arguably introduce new complexities to the multifaceted debate over the scope of the self-defense concept. Ideally, it should be possible to convene a global international conference to consider whether the advent of cyber attacks has created a need for revision of the *jus ad bellum* or the *jus in bello*. But as I have tried to demonstrate in another forum, it has proven very difficult in today's environment for an international conference to conclude a global treaty to resolve challenges in the most important areas of international relations.[79] In the area of the law of armed conflict, there is considerable concern that any major treaty that would result from a global conference would undermine rather than improve the current law.[80]

---

76. *See* Christopher Greenwood, *Self-Defence*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶ 41 (2011), http://www.mpepil.com/sample_article?id=/epil/entries/law-9780199231690-e401&recno=2&.

77. *Id.* ¶ 14.

78. *Id.*

79. *See* MURPHY, *supra* note 5. The five topical areas covered are the maintenance of international peace and security, the law of armed conflict, arms control and disarmament, human rights and international environmental issues.

80. *See id.* at 161–80. *See also* Jean-Philippe Lavoyer, *International Humanitarian Law: Should It be Reaffirmed, Clarified or Developed?*, *in* ISSUES IN INTERNATIONAL LAW AND MILITARY OPERATIONS 287 (Richard B. Jacques ed., 2006) (Vol. 80, U.S. Naval War College

The validity of this concern is demonstrated by recent efforts in international forums to regulate the cyber field, including the possibility of cyber war. Indeed, as suggested in the introduction to this article, these efforts arguably constitute a use of the international legal process in a way that threatens U.S. and other Western States' vital interests. It is to this important issue that the next section of this article turns.

III. EFFORTS TO USE THE INTERNATIONAL LEGAL PROCESS TO REGULATE CYBER ACTIVITIES, INCLUDING CYBER WAR, IN A WAY THAT THREATENS U.S. AND OTHER WESTERN STATES' VITAL INTERESTS

As this article is being written, the *Financial Times* features a full page article on the UN World Conference on International Telecommunications, scheduled to be held in Dubai in December 2012 and sponsored by the ITU, a specialized agency of the United Nations.[81] Although, technically, the conference is supposed to focus on international agreements governing telecommunications, some proposals are expected to stretch broadly into the controversial issue of governance of the Internet. According to the *Financial Times*:

> The battle is already being fought behind closed doors at the International Telecommunications Union. . . . Western nations—such as the US and the EU—in particular do not want to give the ITU extra authority that could indirectly benefit authoritarian regimes in the Middle East, eastern Europe and Asia. They are accused of seeing an opportunity to enhance their ability to control the web and crack down on political dissidents.
>
> "If new governance rules had been set to tighten the control of the web a few years ago we would not have had an Arab spring," says one senior EU diplomat. "The internet must be left free and untouched, the less we tinker with it the better."[82]

There can be little doubt about the validity of the senior EU diplomat's observation that if new governance rules had been in place to tighten control of the web at the time of the Arab spring uprising in the Middle East, it

---

International Law Studies). For a comment on Lavoyer's presentation, see John F. Murphy, *Enforcing the Law*, *in id.* at 311.

81. *See* Daniel Thomas, Richard Waters & James Fontanella-Klan, *The Internet: Command and Control*, FINANCIAL TIMES (London), Aug. 28, 2012, at 5.

82. *Id.*

would never have taken place, or at a minimum would not have enjoyed the success it did. His observation also illustrates an example of a possible connection between efforts to gain control of the Internet and cyber war. It will be remembered that the Arab Spring led to initial violence in Egypt, a civil war in Libya that, with the aid of NATO air coverage, resulted in a regime change, and to the extreme violence in Syria. A major goal of Russia and China—the leaders in the effort to issue regulations that would put limits on use of the Internet—is to ensure that they will not be subject to uprisings like the Arab Spring that result in regime change. Their hard line against Western efforts in the UN Security Council to impose stringent economic sanctions or other forceful measures against the Assad government in Syria in the name of the responsibility to protect illustrates how far they are opposed to the entire concept of forceful regime change.[83]

Russia and China have been pressing their efforts to achieve international regulation of the Internet for some time now. For example, by letter of September 12, 2011, Russia, China, Tajikistan and Uzbekistan, transmitted an International Code of Conduct for Information Security to the UN Secretary-General.[84] The United States and other countries' responses to this proposal have been lukewarm at best, and the United States has been consistent in its resistance to proposals calling for control of the Internet passing to a UN agency.[85] For example, Terry Kramer, the U.S. Ambassador to the Dubai conference, has been reported as saying that

> [t]he US is concerned that proposals by some other governments could lead to greater regulatory burdens being placed on the international telecom sector, or perhaps even extended to the internet sector. The United States also believes that existing multi-stakeholder institutions, incorporating industry and civil society, have functioned effectively and will continue to ensure the health and growth of the internet and all its benefits.[86]

---

83. For discussion of the Arab spring and the responsibility to protect, see John F. Murphy, *Responsibility to Protect (R2P) Comes of Age? A Sceptic's View*, 18 ILSA JOURNAL OF INTERNATIONAL & COMPARATIVE LAW 413 (2012).

84. For text of the code, see Letter dated September 12, 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, Annex, U.N. DOC. A/66/359 (Sept. 14, 2011).

85. *See* Leo Kelion, *US Resists Control of Internet Passing to UN Agency*, BBC NEWS TECHNOLOGY (Aug. 3, 2012, 9:13 PM), http://www.bbc.co.uk/news/technology-19106420.

86. *Id.*

Similarly, according to a recently released document, "[t]he United States will oppose efforts to broaden the scope of the ITRs (International Telecommunication Regulations) to empower any censorship of content or impede the free flow of information and ideas."[87]

In sharp contrast, during a meeting in 2011 between then Russian Prime Minister Vladimir Putin and ITU Secretary-General Dr. Hamadoun Touré, Putin reportedly told Touré that Russia was keen on the idea of "establishing international control over the Internet using the monitoring and supervisory capability of the International Telecommunications Union."[88] It is hardly surprising that countries like China and Iran would support Putin's proposal.[89] But it is at least disappointing to learn that democratic countries like Brazil and India reportedly "share the belief that the Geneva-based UN agency the International Telecommunications Union (ITU) would do a better job if put in charge of international cyber-security, data privacy, technical standards and the global web address system."[90]

In response to the Russian challenge, "at least within the U.S., condemnation of the ITU's dangerously amateurish behavior has been universal. Republican and Democrats, Congress, the White House and the FCC [Federal Communications Commission], along with major industry representatives, consumer advocates, and engineering groups including the highly-respected and international Internet Society, have all raised alarms over both the content and the process of upcoming negotiations."[91] For its part, on April 19, 2012, the U.S. House of Representatives received a draft resolution whereby it was

> the sense of the House of Representatives that if a resolution calling for endorsement of the proposed international code of conduct for information security or a resolution inconsistent with the principles above comes up for a vote in the United Nations General Assembly or other international organization, the Permanent Representative of the United

87. *See* Larry Downes, *Why is the UN Trying to Take over the Internet?,* FORBES (Aug. 9, 2012), http://www.forbes.com/sites/larrydownes/2012/08/09/why-the-un-is-trying-to-take-over-the-internet/.

88. *Id.*

89. *Id.*

90. *See Russia Calls for Internet Revolution*, RT QUESTION MORE (May 28, 2012), http://rt.com/news/itu-internet-revolution-russia-386/.

91. *See* Downes, *supra* note 87.

> States to the United Nations or the United States representative to such other international organization should oppose such a resolution.[92]

At this writing, the draft resolution has been referred to the House Committee on Foreign Affairs but no further action has been taken on it.

It remains to be seen what will happen in December at the conference in Dubai. One possibility is that the meeting could prove inconclusive. Although each of the 193 countries expected to attend the meeting will have a vote, and the United States and like-minded countries could therefore be outvoted, Dr. Toure' reportedly has insisted that there will be no votes at the conference and no proposal will be passed without consensus.[93] It may be impossible to reach consensus, however, on the controversial governance proposals, and if so, there is a good chance that action on them will be postponed at least for a year.[94]

It remains to be considered whether it would be a good idea to try to reach an agreement on the terms of an arms control treaty on cyber weapons. In its July 1, 2010 issue, the *Economist* noted that Russia had engaged in "longstanding calls for a treaty."[95] Surprisingly, the *Economist* also reported that General Keith Alexander, who heads U.S. Cyber Command, had welcomed the Russian initiative as a "starting point for international debate."[96] The report is surprising because the United States has resisted Russian calls for an arms control treaty on cyber war,[97] and there is no indication that U.S. policy on this subject has changed.

There are several possible reasons for the U.S. resistance to Russian calls for a treaty on cyber war. For one thing, nation-States have differing views on what constitutes cyber-warfare. Most advanced democracies see cyber attacks as "an assault on the computer infrastructure that underlies power, telecommunications, transportation and financial systems."[98] Russia, however, prefers to call cyber warfare an "information war" and has introduced a resolution in the United Nations every year since 1998 calling for a

---

92. H. R. Res. 628, 112th Cong. (2012).

93. *See* Thomas, Waters & Fontanella-Khan, *supra* note 81.

94. *Id.*

95. *See Cyberwar: It is Time for Countries to Start Talking about Arms Control on the Internet*, ECONOMIST, July 3, 2010, at 11, *available at* http://www.economist.com/node/16481504.

96. *Id.*

97. *See e.g.*, Tom Gjelten, *Seeing the Internet as an "Information Weapon*," NPR (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.

98. *Id.*

treaty outlawing "information terrorism."[99] According to Russian Defense official Sergei Korotkov, "anytime a government promotes ideas on the Internet with the goal of subverting another country's government—even in the name of democratic reform—it should qualify as 'aggression.'"[100]

In its article on "Cyberwar," the *Economist* suggests that the United States has

> resisted weapons treaties for cyberspace for fear that they could lead to rigid global regulation of the internet, undermining the dominance of American internet companies, stifling innovation and restricting the openness that underpins the net. Perhaps America also fears that its own cyberwar effort has the most to lose if its well-regarded cyberspies and cyber-warriors are reined in.[101]

At the same time, the *Economist* acknowledges another, perhaps more compelling, reason for U.S. hesitation: "a START-style treaty may prove impossible to negotiate. Nuclear warheads can be counted and missiles tracked. Cyber-weapons are more like biological agents; they can be made just about anywhere."[102]

As noted by Michael Schmitt in 1999, military thinkers devised and developed a term—information operations (IO)—anticipating this "new category of warfare" that grows from the Internet's interconnectivity and other new forms of communications.[103] In the same year, the U.S. Department of Defense Office of General Counsel rejected calls for IO-specific rules as "premature", arguing, *inter alia*, that in regulating IO via the law of war, the "process of extrapolation appears to be reasonably predictable."[104] Perhaps more surprisingly, in light of its generally favoring the development of new norms in the law of war, in 2003, the International Committee for the Red Cross expressed the view that "the existing legal framework is on the whole

---

99. *Id.*

100. *Id.*

101. *See Cyberwar*, *supra* note *95*.

102. *Id.*

103. *See* Schmitt, *Computer Network Attack and the Use of Force in International Law*, *supra* note 11, at 890.

104. Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (2d ed. Nov. 1999), *reprinted in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 31, at 459, 475 ("There seems to be no particularly good reason for the United States to support negotiations for new treaty operations in most of the areas of international law that are directly relevant to information operations." *Id.* at 522.).

adequate to deal with present day international armed conflicts."[105] Writing in 2007, Duncan Hollis stated that "[a] majority of military thinkers agree, arguing in favor of an analogy approach or decrying the possibility of IO-specific rules as premature or unrealistic."[106] It appears that a majority of military thinkers and U.S. government officials are still opposed to the negotiation of a new international convention on cyber war.[107] There is greater support for the negotiation of such a convention among civilian academic writers.[108] In my view, the arguments in favor of this view have considerable cogency and might well carry the day if the circumstances of today's world were more favorable to this possibility.[109] But they are not.

I have already noted the difficulty involved in trying to conclude a global treaty to resolve challenges in the most important areas of international relations, including the law of armed conflict.[110] The difficulties and the risks may be especially severe in the areas of maintenance of interna-

---

105. INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 4 (2003), *available at* http://www.icrc.org/eng/assets/files/other/ihlcontemp_armedconflicts_final_ang. pdf.

106. See Duncan B. Hollis, *Why States Need An International Law For Information Operations*, 11 LEWIS & CLARK LAW REVIEW 1023, 1038–39 n.65 (2007).

107. Recently, Steven G. Bradley, who served for almost five years as the head of the Office of Legal Counsel in the Department of Justice during the George W. Bush administration, and had "occasion to advise on cybersecurity issues" during his tenure, stated categorically that:

> In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwar—perhaps a kind of arms control agreement for cyber weapons. I believe there is no foreseeable prospect that this will happen. Instead, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations. And the policy decisions made by the United States in response to particular events will have great influence in shaping those international norms. I think that's the way we should want it to work.

Steven G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Operations*, 2 HARVARD NATIONAL SECURITY JOURNAL 591, 611 (2011).

108. *See, e.g.*, Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 JOURNAL OF THE NATIONAL ASSOCIATION OF ADMINISTRATIVE LAW JUDICIARY 602 (2011) (who favors the negotiation of such a convention, but also cites and discusses both writers who favor and those who oppose the negotiation of such a convention).

109. In particular, I find the arguments of Hollis, *supra* note 106, to be quite persuasive. Hollis, currently a professor at Temple University School of Law, spent six years in the Office of the Legal Adviser, U.S. Department of State, before going into academia.

110. *See supra* notes 79 and 80 and associated textual discussion.

tional peace and security[111] and the law of armed conflict.[112] This is because the world has become increasingly hostile to the values and interests of Western democracies and nation-States increasingly prone to negotiate on a zero-sum basis.[113] Russia and China, States that have progressively assumed leadership roles in this new environment, are dictatorships hostile to the United States in particular, and so-called emerging powers such as India, Brazil and Turkey are "not ready for prime time."[114] In such an environment, the negotiation of an international convention on cyber war would indeed seem "premature."

If it is "premature" to try to negotiate an international convention on cyber war, are there other steps that might be taken to mitigate some of the problems posed by cyber threats? It is worth noting that the *Economist* writing in 2010 noted the difficulties of negotiating "a START-style treaty"[115] and suggested instead that "countries should agree on more modest accords, or even just informal 'rules of the road' that would raise the political cost of cyber-attacks."[116]

The *Economist*'s reference to informal rules of the road raises the controversial issue of so-called "soft law." The term "soft law" is controversial because various commentators, including this one, believe that use of the term creates confusion, especially because there is no agreement on what the term "soft law" means, and therefore is unhelpful.[117] One definition of soft law would include non-binding guidelines or even rules of the road. In some instances, especially in the fields of human rights or international environmental law, such guidelines are a step toward the eventual conclusion of a binding treaty. But, as I have stated elsewhere, use of the term soft law is "especially unfortunate when, as is arguably increasingly the case, legally nonbinding international instruments are utilized not as part of the process of making international law but rather as an alternative to it . . . because of the perception that application of legally binding international norms would not be appropriate under the circumstances."[118]

---

111. *See* MURPHY, *supra* note 5, at 103–60.

112. *Id.* at 161–80.

113. *See especially* IAN BREMMER, EVERY NATION FOR ITSELF (2012).

114. *See* Fareed Zakaria, *A Post-American World in Progress: Why Emerging Powers Didn't Lead in 2011 and Won't in the Coming Year*, TIME, Jan. 9, 2012, at 17.

115. *See Cyberwar, supra* note 95.

116. *Id.*

117. For my views on this controversy, see MURPHY, *supra* note 5, at 20–23.

118. *Id.* at 22–23.

In addition to recognizing the possibility of establishing "a set of non-legally binding norms with the expectation that international legal rules will emerge from them in time,"[119] Duncan Hollis has suggested that

> the path to creating international law need not always occupy the global stage. Perhaps the starting point for ILIO [international law for information operations], like the law of war itself, might best lie in one or more individual nation-states producing a set of self-governing rules for their own IO. Or, a group of interested states might decide to articulate an ILIO among themselves, as the Council of Europe did for Cybercrime . . . .[120]

However States may decide to approach the problems posed by cyber war, they will have to cope with the special challenges created by the increasingly global operations of terrorist groups like Al Qaeda. We turn to a consideration of these challenges in the next section of this article.

IV. TERRORISM AND CYBER WAR

The literature on terrorism is vast, but there is no need discuss it in this article. Rather, for present purposes, the focus will be on what has been called the "new terrorism."[121] The quintessential example of a group engaged in the new terrorism is Al Qaeda, and the quintessential example of a new terrorism act is the horrific attacks of September 11, 2001. With respect to the old terrorism, the conventional wisdom suggested that terrorists had little interest in killing large numbers of people. The perception was that large scale killings would undermine their efforts to gain sympathy for their cause, which was usually to overthrow the government of a particular country (e.g., Germany or Italy). In sharp contrast, an especially disquieting aspect of the new terrorism is the increased willingness of terrorists to kill large numbers of people. For example, the terrorist attacks in the United States on September 11, 2001 killed 2,973 people; in Madrid on March 11, 2004, attacks killed 191 and wounded 2,050; and in the bombings in the Mumbai (Bombay) train system on July 11, 2006, they killed 209

119. *See* Hollis, *supra* note 106, at 1059.

120. *Id.*

121. *See, e.g.*, John F, Murphy, *Challenges of the "New Terrorism," in* ROUTLEDGE HANDBOOK OF INTERNATIONAL LAW 281, 283–86 (David Armstrong ed., 2009).

and injured more than 700.[122] Jeffrey D. Simon has aptly pinpointed a major cause of the radical change in attitude:

> Al Qaeda . . . is representative of the emergence of the religious-inspired terrorist groups that have become the predominate form of terrorism in recent years. One of the key differences between religious-inspired terrorists and politically motivated ones is that the religious-inspired terrorists have fewer constraints in their minds about killing large numbers of people. All nonbelievers are viewed as the enemy, and the religious terrorists are less concerned than political terrorists about a possible backlash from their supporters if they kill large numbers of innocent people. The goal of the religious terrorist is transformation of all society to their religious beliefs, and they believe that killing infidels or nonbelievers will result in their being rewarded in the afterlife. Bin Laden and Al Qaeda's goal was to drive U.S. and Western influences out of the Middle East and help bring to power radical Islamic regimes around the world. In February 1998, bin Laden and allied groups under the name "World Islamic Front for Jihad Against the Jews and the Crusaders" issued a fatwa, which is a Muslim religious order, stating that it was the religious duty of all Muslims to wage a war on U.S. citizens, military and civilian, anywhere in the world.[123]

Another facet of the new terrorism is the extraordinary extent to which terrorists have developed global networks. A recent study finds that Al Qaeda operates in a network that spans roughly one hundred countries, including the United States.[124] While that network has weakened severely in recent years with the assassination or capture of key Al Qaeda leaders such as Osama bin Laden, the Al Qaeda organization has simultaneously gained many new militants to its cause through a "terror by franchise" approach.[125] That is, while the jihadi threat has been suppressed in some countries (e.g., Saudi Arabia and Indonesia) it is increasing in places in North Africa and Lebanon. Groups inspired by Al Qaeda have in turn established links with a new breed of home-grown terrorist. The problem is especially acute in

---

122. *See* BETH VAN SCHAACK & RONALD C. SLYE, INTERNATIONAL CRIMINAL LAW AND ITS ENFORCEMENT 615 (2d ed. 2010).

123. Jeffrey D. Simon, *The Global Terrorist Threat,* 82 PHI KAPPA PHI FORUM 10, 11 (2002).

124. Jayshree Bajoria & Greg Bruno, *al-Qaeda (a.k.a. al-Qaida, al-Qa'ida),* http://www.cfr. org/publication/9126/ (last updated June 6, 2012).

125. *See, e.g.*, Farhan Bokhari & Stephan Fidler, *Rivalries Rife in Lair of Leaders*, FINANCIAL TIMES (London), July 5, 2007, at 5.

the United Kingdom, where radicalized British Muslims have established links with Al Qaeda and Taliban-sponsored training camps in Pakistan.[126] In continental Europe, home grown terrorists have established links with radical cells in North Africa.

The concern that terrorists may resort to the use of weapons of mass destruction—nuclear, chemical, or biological—is long standing.[127] Since September 11, however, this concern has been greatly heightened. Moreover, Osama bin Laden and Al Qaeda made plain on numerous occasions their desire to obtain weapons of mass destruction, especially nuclear weapons, and their use of civilian aircraft on September 11 and their effective employment of the Internet since then have demonstrated their technological competence. Their proficiency with computers has led one commentator to suggest that they now have the capacity for hijacking satellites: "Capturing signals beamed from outer space [it is alleged] terrorists could devastate the communications industry, shut down power grids, and paralyze the ability of developed countries to defend themselves."[128]

Interestingly, there appears currently to be a tendency to play down the risk of terrorists being engaged in a cyber war, on the ground that today's cyber attacks are so sophisticated that they require a State government to carry out rather than individual terrorists or terrorist organizations operating on their own.[129] This view may be too complacent, however.[130] Certain-

126. *See* Stephen Fidler, *Radicalising Wave Crosses the Atlantic*, FINANCIAL TIMES (London), July 5, 2007, at 5.

127. *See* Brian M. Jenkins & Alfred P. Rubin, *New Vulnerabilities and the Acquisition of New Weapons by Nongovernmental Groups*, *in* LEGAL ASPECTS OF INTERNATIONAL TERRORISM 221 (Alone E. Evans & John F. Murphy eds., 1978).

128. *See* Lawrence Wright, *The Terror Web*, NEW YORKER, Aug. 2, 2004, at 40, 50, *available at* http://www.newyorker.com/archive/2004/08/02/040802fa_fact.

129. *See e.g.*, Richard, *supra* note 19, at 854 (where the author notes that the sophistication of the Stuxnet virus is so great that "it could have taken five to ten programmers upwards of six months to create Stuxnet" and therefore it is likely that a government or governments is behind it rather than individual hackers). *See also* Charles J. Dunlap Jr., *Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy, in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 31, at 353, 359 (arguing that the absence of any catastrophic events caused by IO demonstrates that IO may be more difficult to accomplish than theorists realize, but conceding that IO still poses a threat in certain contexts, such a IO's capacity to steal identities).

130. For example, during its 2006 armed conflict with Israel, Hezbollah, which the United States and Israel have labeled a terrorist organization, reportedly engaged in cyber war against Israel. According to the report,

> While fighting raged in the towns and hills of southern Lebanon, Hizbullah launched an all-out assault on Israeli civilian and military communications networks. Hizbullah hackers

ly the computer capability demonstrated by Al Qaeda is sufficient to allow it to be intensively involved in cyber espionage, and as to mounting a cyber attack that would result in a large number of deaths and major property damage, there is an increasing risk that State adversaries of the United States and other Western democracies might give the support to terrorist groups necessary to allow them to engage in such a cyber attack. For example, Iran might give such support to Al Qaeda, and certain elements of the Pakistani government might do the same with the Taliban and Al Qaeda.

As is well known, a major challenge in defending against a cyber attack is the problem of attribution, i.e., determining where the attack came from and who or what engaged in it. The problem of attribution is greatly compounded when a cyber attack is engaged in by a terrorist organization like Al Qaeda that is globally networked in over a hundred countries. In considering the feasibility of developing a customary ILIO, Hollis argues that

> attribution issues may make it difficult to ever discern state practice in IO. IO's strength often lies in its anonymity and secrecy—victims of IO may not know that they have been subjected to it, let alone who is responsible (although constantly changing technology ensures that this will not always be the case).[131]

Hollis also cautions that "it can take years or decades for state practice to coalesce into customary international law."[132] Moreover, it should be noted, dramatic changes in the nature of international relations have made the process of creating customary international law particularly problematic.[133]

> shut down Israeli phone systems, electric grids, and IT systems periodically throughout the war. At the same time, they hacked into phone lines and eavesdropped on Israeli conversations, including those of Israeli soldiers, who, in many instances, gave away important tactical information on phone calls home. The hackers even cracked encrypted Israeli military communications, providing the militants with information on Israeli movements and intentions. Through electronic warfare, Hizbullah made life even more difficult in northern Israel and, at the same time, gained valuable, tactical intelligence on its enemies.

Andrew Chadwick, *The 2006 Lebanon War: A Short History, Part II*, SMALL WARS JOURNAL 5 (Sept. 12, 2012), http://smallwarsjournal.com/jrnl/art/the-2006-lebanon-war-a-short-history-part-ii (citation omitted).

131. *See* Hollis, *supra* note 106, at 1054.

132. *Id.*

133. For discussion and citations, see MURPHY, *supra* note 5, at 16–19.

It is at least arguable that the threats to States are no longer primarily from other States, but from non-State actors. If this is the case, Hollis asks, "do we serve international peace and security by imposing so many restrictions on how states use IO against non-state actors."[134] Answering his question in the negative, Hollis continues:

> For example, rather than seeing ILIO as essentially a question of restricting what States do to one another, ILIO could establish rules enabling states to better meet the challenges posed by non-state actors, particularly those bent on global terror. In the language of economists, ILIO may reduce the transaction costs that states face in combating transnational terrorism. The current system—which might prohibit a state from responding to an al-Qaeda attack from Pakistan directly or immediately, requiring it instead to ask Pakistan for assistance—is not terribly efficient and may have high costs for the victim state's safety and security. In its place, ILIO offers an opportunity for states to acknowledge their collective interest in combating non-state terrorist actors as a threat to the state system itself, and to devise cooperative mechanisms that increase the efficiency of such efforts. This might involve, for example, states such as Pakistan consenting to suspend the non-intervention principle in certain pre-agreed circumstances and allowing injured states to respond immediately and directly to IO generated from their territory (i.e., to conduct an active defense to CNA). Or, perhaps states could establish a program where a state sends information officers to other states who can approve IO methods that target or transit the sending state's territory. There is already some precedent for this in the maritime context, through the practice of "shiprider" agreements, in which a foreign state agrees that one of its officials may serve abroad a U.S. ship and authorize it to conduct law enforcement activities against ships of that foreign state and even within the foreign state's territorial seas.[135]

Hollis's remarks are intriguing. They posit, correctly in my view, that even adversarial States, for example, Russia and the United States, may have a common interest in agreeing upon rules, perhaps informal in nature, that allow them to cooperate in employing IO in combating global terrorism. The proposition that cooperation between Pakistan and the United States in combating IO by terrorists is possible may be a bit more problematic in light of evidence of Pakistan's Inter-Services Intelligence Directorate assisting the Taliban in Afghanistan in their use of improvised explo-

134. Hollis, *supra* note 106, at 1055.
135. *Id.* at 1055–56.

sive devices against members of the Afghanistan government and coalition forces.[136] But even in this case, Pakistan might be more amenable to cooperating with the United States in using IO to response to Taliban or Al Qaeda attacks launched from Pakistan into Afghanistan than it has been with respect to drone attacks launched by the United States into Pakistan against the Taliban or Al Qaeda.

In any event, at a minimum efforts to reach informal "rules of the road" regarding the use of IO against global terrorism would seem warranted. There seems little doubt that the greatest national security threat facing the United States and its allies in the coming years is asymmetric warfare, of which cyber warfare is a prime example.

V. CONCLUSION

To answer the question posed in the title of this article, i.e., whether the international legal process may constitute a threat to U.S. vital interests in the area of cyber war and international law, the answer is it may unless the United States and its allies resist efforts by Russia and other like-minded States to establish international regulation of the Internet that would benefit authoritarian regimes and endanger basic values such as freedom of speech and privacy. Similar efforts by Russia in particular to conclude a treaty on cyber war that could undermine the United States and other Western States' national security must also be resisted. At the same time, at least with respect to cyber war and international law, it may be desirable to engage in more modest steps, such as considering possible non-binding guidelines, either as a first step toward an eventual binding treaty or as a substitute for such a treaty.

Although the conventional wisdom that holds that traditional espionage is not regulated by international law, with the exception that persons prosecuted for espionage under national law are entitled to due process under international human rights law, the recent emergence of cyber espionage utilizing extraordinarily effective computer viruses such as Flame and Gauss may require a rethinking of the conventional wisdom. Admittedly, reaching agreement on the rules of international law that would govern cyber espionage might be an impossible mission.

---

136. *See* John F. Murphy, *Mission Impossible? International Law and the Changing Character of War*, 41 ISRAEL YEARBOOK ON HUMAN RIGHTS 1, 4 (2011).

When all is said and done, it is highly likely that the legal issues surrounding cyber war and related cyber activities are not the most important challenge facing the United States and its allies. If Richard Clarke is right that although the United States has developed a so far unmatched capacity to conduct an offensive cyber war, it has virtually no *defense* against the cyber attacks he says are targeting us now, and will be in the future;[137] the greater urgency is to remedy this situation. A major obstacle to resolving this problem is the resistance of private industry to governmental efforts to induce businesses to improve their cyber security. It is clear, however, that government and private business cooperation will be indispensable if U.S. defenses against cyber attack are going to be effective.

137. *See supra* note 71 and associated text.