2014

Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law

Jack M. Beard
University of Nebraska College of Law, jbeard2@unl.edu

47 Vanderbilt Journal of Transnational Law 67 (2014)

Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law

Jack M. Beard[*]

ABSTRACT

Reports of state-sponsored harmful cyber intrusions abound. The prevailing view among academics holds that if the effects or consequences of such intrusions are sufficiently damaging, international humanitarian law (IHL) should generally govern them—and recourse to armed force may also be justified against states responsible for these actions under the jus ad bellum. *This Article argues, however, that there are serious problems and perils in relying on analogies with physical armed force to extend these legal regimes to most events in cyberspace. Armed conflict models applied to the use of information as a weapon and a target are instead likely to generate "legal phantoms" in cyberspace—that is, situations in which numerous policy questions and domestic criminal issues are often misinterpreted as legal problems governed by the IHL framework or the* jus ad bellum. *This Article assesses this dilemma in the context of four key problem areas relating to dimensions of information: (1) problems of origin, organization, and availability; (2) problems of access and control; (3) problems of exploitation; and (4) problems of manipulation and content.*

---

* Assistant Professor of Law, University of Nebraska College of Law; former Associate Deputy General Counsel (International Affairs), Department of Defense. The author greatly appreciates helpful comments by Duncan Hollis, Matthew Schaefer, Brian Lepard, and Richard Moberly on earlier drafts.

TABLE OF CONTENTS

It has long been clear that private persons and state-sponsored actors can cause damage by transmitting information through cyberspace (to disrupt, exploit, manipulate, or deny access to data in other computer systems and networks) and that such actions pose a

real threat to businesses and governments.[1] While cybercrime, state-sponsored hostile cyber acts, and diverse types of cyber mischief are common, the world has not yet experienced a "cyberwar."[2] In spite of dire, repeated predictions to the contrary, a cyberwar (an armed conflict limited to cyber actions alone) may in fact be unlikely.[3]

Yet regardless of how conflict and competition in cyberspace may be characterized, military organizations have concluded that cyberspace is in fact a new contested "domain" for military operations (joining the land, maritime, air, and space domains), and some have announced their intention to achieve "superiority" in it.[4] This willingness to apply a traditional model of military operations is based on the assumption that conflict in cyberspace represents an extension of conflict in physical domains, and therefore, actions taken in this realm should generally be subject to the same rules and approaches that apply to the employment of "kinetic capabilities."[5]

---

1. For example, cyber threats have reportedly forced the U.S. government to spend vast sums on cyber defense and operations. *See* Barton Gellman & Greg Miller, *U.S. Spy Network's Successes, Failures and Objectives Detailed in 'Black Budget' Summary*, WASH. POST, Aug. 29, 2013, at A1 (noting that leaked reports show how the U.S. government now budgets several billion dollars a year on "conducting cyber operations").

2. *See* JAMES ANDREW LEWIS, CTR. FOR STRATEGIC AND INT'L STUDIES, THE CYBER WAR HAS NOT BEGUN 1 (2010), *available at* http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf ("We are not in a 'cyber war'. War is the use of military force to attack another nation and damage or destroy its capability and will to resist. Cyber war would involve an effort by another nation or a politically motivated group to use cyber attacks to attain political ends. No nation has launched a cyber attack or cyber war against the United States.").

3. *See* Thomas Rid, *What Would a Real Cyberwar Look Like?*, NEW SCIENTIST (Sept. 15, 2013), http://www.newscientist.com/article/mg21929334.800-why-a-cyberwar-wont-happen.html#.Uqx02bQsrlI ("Never has a human been injured or hurt as an immediate consequence of a cyberattack. Never did a state coerce another state by cyberattack. Very rarely did state-sponsored offenders take credit for an attack. So if we're talking about war – the real thing, not a metaphor, as in the 'war on drugs' – then cyberwar has never happened in the past, is not taking place at present, and seems unlikely in the future.").

4. *See, e.g.*, U.S. DEP'T OF THE AIR FORCE, CYBERSPACE OPERATIONS AIR FORCE DOCTRINE DOCUMENT 3-12, at 37 (amended Nov. 11, 2011) [hereinafter AIR FORCE, CYBERSPACE OPERATIONS] ("[A] culture shift is underway that reflects the reality that cyberspace is a contested domain and the importance of maintaining cyberspace superiority.").

5. A U.S. DoD policy report noted that

> [i]nternational legal norms, such as those found in the UN Charter and the law of armed conflict, which apply to the *physical domains* (i.e., sea, air, land, and space), also apply to the cyberspace domain. . . . If directed by the President, DoD will conduct offensive cyber operations in a manner consistent with the policy principles and legal regimes that the Department follows for *kinetic capabilities*, including the law of armed conflict. (emphasis added).

See, e.g., U.S. Dep't of Def., Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, at 5, 9 [hereinafter DoD Cyberspace Policy Report].

The feared arrival of a new epoch of cyber warfare and the decision by military organizations to treat cyberspace as a new operational military domain have been accompanied by an eagerness to view the law of armed conflict or the *jus in bello* (also referred to as international humanitarian law or IHL) as the appropriate legal framework to govern many cyber operations, particularly those conducted in response to so-called cyber attacks.[6]

The decision to apply the IHL framework to events in cyberspace may appear to be an easy one, drawing on the perceived similarity of the effects of cyber operations and those of conventional military operations in physical domains. For example, a former U.S. military official has suggested that "a cyberattack is governed by basically the same rules as any other kind of attack if the effects of it are essentially the same."[7] It is thus not surprising that military organizations have proceeded to equate many conventional and cyber operations, concluding for example that "[t]he fundamental targeting issues arising are no different in cyber operations as compared to those applicable to kinetic targeting."[8]

By viewing conflict in cyberspace as an extension of conflict in physical domains and by emphasizing the apparent similar effects of cyber and conventional weapons, the IHL framework becomes by default the appropriate lens for assessing many hostile cyber acts. This Article argues, however, that due to the unusual properties of information itself, there are serious problems and perils in relying on such analogies to extend the IHL framework to most events in cyberspace.

Rather than being easily governed by a broad application of the IHL framework, the use of information as a weapon and a target will more often be highly problematic. Armed conflict models are likely to generate "legal phantoms" in cyberspace—that is, situations in which numerous policy questions, domestic criminal issues, and technological challenges are misinterpreted as legal problems governed by the IHL framework or that implicate the *jus ad bellum*. (This latter body of international law—which is prominently reflected in obligations in the United Nations Charter—governs recourse to

---

6. *See* David Sanger & Elisabeth Bumiller, *Pentagon to Consider Cyberattacks Acts of War*, N.Y. TIMES, June 1, 2011, at A10 (citing General Kevin P. Chilton, the head of U.S. Strategic Command, as saying that "in the event of a cyberattack 'the law of armed conflict will apply'").

7. *See* S. Gorman & J. Barnes, *Cyber Combat: Act of War*, WALL ST. J., May 31, 2011, at A1 (quoting Charles Dunlap, a retired Air Force Major General).

8. *See, e.g.*, U.S. DEP'T OF THE AIR FORCE, AIR FORCE OPERATIONS AND THE LAW 99 (2d ed. 2009) (noting that, if an armed conflict is present, the "fundamental targeting issues arising are no different in cyber operations as compared to those applicable to kinetic targeting").

armed force, as opposed to the IHL regime, which governs the way warfare is conducted.)[9]

As examined in this Article, the clear reluctance by states to apply these rules to cyber incidents, standing alone, is prudent. There is an underappreciated and significant danger in broadly applying the IHL framework to diverse areas of state-sponsored competition and conflict.[10] This is particularly true with respect to the application of IHL principles and obligations, as well as the *jus ad bellum*, to the many diverse uses and dimensions of information in cyberspace.

The IHL framework and the *jus ad bellum* nonetheless continue to be advanced as appropriate legal frameworks to fill perceived gaps in existing legal coverage of cyberspace, particularly in an environment where even the U.S. secretary of defense warns of a "cyber Pearl Harbor," in which catastrophic physical damages are caused by a future cyber attack.[11] However, such hypothetical, devastating, and stand-alone cyber attack scenarios remain highly unlikely from several different perspectives.[12] The reality of the current cyber threat is much different—it is informational in nature, characterized by diverse and increasingly complex cyber actions involving the disruption, exploitation, manipulation, or damage of data.

Current state practice reflects this more complex reality, since no state has actually invoked and applied IHL rules or the *jus ad bellum* to any hostile cyber act standing alone (nor actually engaged in cyberwar). In practice, cyberwar is in fact still a theoretical concept, and states have thus not yet applied an effects-based approach to real cyber incidents, nor have they done so based exclusively on analogies

---

9. *See* ANTHONY CLARK AREND & ROBERT J. BECK, INTERNATIONAL LAW AND THE USE OF FORCE 2 (1993) (describing the *jus ad bellum* as "the rules of international law relating to the recourse to force" and "the norms that determine when the state may permissibly resort to force against another state").

10. *See* Int'l Comm. of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflict*, 89 INT'L REV. OF THE RED CROSS 719, 726 (2007) [hereinafter *International Humanitarian Law*] (noting that because of the more flexible standards applicable to the lawful taking of life and the detention of persons in armed conflicts, "it is both dangerous and unnecessary, in practical terms, to apply IHL to situations that do not amount to war. This is not always fully appreciated.").

11. *See* Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES, Oct. 12, 2012, at A1 (warning that "the United States was facing the possibility of a 'cyber-Pearl Harbor' and was increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks and government").

12. *See, e.g.*, Thomas Rid, *Cyber War Will Not Take Place*, 35 J. STRATEGIC STUD. 5, 10 (2012) ("If the use of force in war is violent, instrumental, and political, then there is no cyber offense that meets all three criteria."); John Arquilla, *Panetta's Wrong About a Cyber 'Pearl Harbor': The Internet Doesn't Work that Way*, FOREIGN POL'Y (Nov. 19, 2012), http://www.foreignpolicy.com/articles/2012/11/19/panettas_wrong_about_a_cyber_pearl_harbor#sthash.xHDb0d4d.dpbs.

drawn from the use of conventional weapons in the physical world.[13] As examined in this Article, the more nuanced and reluctant approach taken by states instead reflects both practical considerations and serious legal concerns, the latter being integrally linked to fundamental problems posed by information as a weapon and target. Cyber operations must thus be contrasted with conventional military operations, which involve weapons-employing physical forces and objects, including (but not limited to) those employing kinetic energy.[14]

While it is possible to characterize various types of information as "cyber weapons" and various data sets (including those connected to physical objects) as "targets," these uses of information raise many issues that are much different than those presented by the use of conventional weapons against physical targets. The wholesale importation of the IHL framework and the *jus ad bellum* into the world of cyber conflicts thus risks ignoring problematic and legally significant dimensions of information.

This Article examines the impact of these dimensions of information on the IHL framework and the *jus ad bellum* when they are applied to conflicts and competition in cyberspace and contrasts them with the application of IHL rules in conventional conflicts in physical domains. These dimensions of information are assessed in the context of four key problem areas as they relate to the use of information as a weapon and target.

These problem areas, which are examined in Parts I through IV of this Article, are (1) problems of origin, organization, and availability; (2) problems of access and control; (3) problems of exploitation (and related challenges to effects-based legal thresholds); and (4) problems of manipulation (and related questions concerning content and users). A careful assessment of these problem areas calls into question the general application of the IHL framework and the *jus ad bellum* to conflicts in cyberspace and also challenges supporting theories that focus on effects-based analogies with

---

13. *See Taking the Mystery Out of Cyberwar*, WASH. POST (June 16, 2013), http://articles.washingtonpost.com/2013-06-16/opinions/40013015_1_stuxnet-effects-consequences ("Although the military has designated cyberspace as a new domain of conflict, there hasn't been a real cyberwar yet. Much about this kind of conflict among nations or groups is still only conjecture.").

14. While the terms *kinetic* and *physical* are sometimes incorrectly used interchangeably, a more accurate definition of the term *kinetic* for targeting purposes refers to "actions that involve the forces and energy of moving bodies, including physical damage to or destruction of targets through use of bombs, missiles, bullets, and similar projectiles." *See* UNITED STATES AIR FORCE, TARGETING AIR FORCE DOCTRINE DOCUMENT 2-1.9, at 115 (2006). Nonkinetic weapons thus include a variety of weapons such as those that emit directed electromagnetic energy or otherwise "produce effects without direct use of the force or energy of moving objects." *Id.* at 116. As discussed below, unlike cyber capabilities, such nonkinetic weapons employ physical forces and display physical properties.

conventional weapons in physical domains. The Article concludes with further reflections on the inherent difficulties associated with regulating information as a weapon, the problems in broadly analogizing conventional armed conflicts with events in cyberspace, and the critical importance of legal analysis for distinguishing the physical from the informational.

I. INFORMATION AS A WEAPON: PROBLEMS OF ORIGIN, ORGANIZATION, AND AVAILABILITY

A. *The Legal Status of Cyber Capabilities as Potential Weapons*

It is clear that information technologies and new types of information have already had profound consequences for military targeting capabilities on the modern battlefield. For example, conventional weapon systems have benefitted in previously unimaginable ways from guidance systems based on information provided by global-positioning-system satellites. [15] Meanwhile, military commanders have gained access to unprecedented intelligence and surveillance capabilities and transformational real-time data provided by unmanned aerial vehicles.[16]

While the use of new types of information is responsible for dramatic improvements in the targeting capabilities of many conventional weapon systems, the use of information itself, as a cyber weapon, is an evolving new chapter in the long history of warfare. These changes include transformational attack capabilities for the military forces of states as well as new asymmetrical attack capabilities for nonstate actors.[17] For the most advanced military powers, cyber capabilities also create new possibilities for attacking a wide variety of objects that may have previously been considered too difficult to target with highly destructive conventional weapons.[18]

---

15. *See* P.W. SINGER, WIRED FOR WAR 58 (2009) (noting both the key role that GPS guidance systems played in the rise of "smart bombs" and the transformation integration in the mid-1990s of unmanned systems with GPS technology—which a retired U.S. Air Force officer described as "the magic moment" for these systems).

16. *See* Jack M. Beard, *Law and War in the Virtual Era*, 103 AM. J. INT'L L. 409, 417 (2009) (noting the use by U.S. ground forces in Iraq of new, transformational, real-time intelligence capabilities, "especially the full motion video provided by UAVs").

17. *See* William F. Lynn III, *Defending a New Domain—The Pentagon's Cyberstrategy*, 89 FOREIGN AFF. 97, 98–99 (2010) ("[C]yberwarfare is asymmetric. . . . A dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States' global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target.").

18. *See* Eric Talbot Jensen, *Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1166 (2003) (noting that "CNA capability provides an enlarged target list that allows commanders to attack additional targets that they may believe are militarily necessary but previously unreachable").

Diverse types of computer viruses, worms, malware, logic bombs, and other potentially destructive computer programs continue to be developed from a wide spectrum of information resources.[19] Such harmful computer programs could arguably be classified as cyber weapons even if a precise or comprehensive definition of that term remains elusive.[20] Thus, notwithstanding definitional problems, the U.S. Department of Defense (DoD) has reportedly assessed the military utility of various cyber techniques and data packages in order to determine how they should be classified alongside other U.S. military capabilities.[21]

A "weapon" for purposes of the IHL regime is broadly defined under Additional Protocol I to the Geneva Conventions of 1949 as "a weapon, means or method of warfare."[22] This expansive definition ensures that the United States and other countries must seriously consider the legal ramifications of the study, development, acquisition, or adoption of possible cyber techniques, tools, and capabilities that may have military applications.[23]

Because it was not difficult to envision scenarios in which various types of harmful computer programs or other data packages could be directed against the computer systems and networks of an enemy, scholars concluded at an early stage that such information *could* constitute a means or method of warfare (or "arms" for military forces to employ as part of an armed conflict) and thus could be subject to the limitations of the IHL regime.[24]

Beyond this widely stated proposition that the IHL framework *could* be applicable to certain hostile cyber actions, the precise extent

---

19. *See* GEORGE B. DELTA & JEFFREY H. MATSUURA, LAW OF INTERNET § 10.02 (3d ed. 2013) (noting that "[t]he scope of computer security threats continues to expand and diversify" and that "[n]ew security threats continue to emerge"); DOD CYBERSPACE POLICY REPORT, *supra* note 5, at 8 (noting that "[m]ost of the technology used in this context [the development and use of malicious cyber tools] is inherently dual-use, and even software might be minimally repurposed for malicious action").

20. For example, the DoD suggests that "there is currently no international consensus regarding the definition of a 'cyber weapon.'" *Id.*

21. *See* Ellen Nakashima, *Defense Dept. Develops List of Cyber-Weapons*, WASH. POST, June 1, 2011, at A3 (reporting that "[t]he Pentagon has developed a list of cyber-weapons and tools, including viruses that can sabotage an adversary's critical networks" and that this "classified list of capabilities . . . has been approved by other agencies, including the CIA").

22. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, *adopted* June 8, 1977, art. 36, 1125 U.N.T.S. 3 [hereinafter Protocol I].

23. The definition is not only broadly encompassing, but also forward-looking. *See* KNUT DÖRMANN, INT'L COMM. OF THE RED CROSS RES. CTR., APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS 2 (2004), *available at* http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf (arguing that the existence of the standard set forth in Protocol I "is a strong indicator that [its drafters] anticipated the application of its rules to new developments of methods and means of warfare").

24. *Id.*

to which that framework should govern specific actions in cyberspace is much less clear. There currently is no state practice and no consensus regarding the actual application of IHL rules (or any other international legal obligations) to cyber attacks. [25] Conversely, however, it may be argued that there is a widespread and consistent practice by states of *not* applying the IHL regime to events that actually occur in cyberspace.

The unwillingness of states to apply IHL obligations to real actions in cyberspace may also reflect practical and strategic considerations that inhibit any discussion or public review of these actions, since states tend to shroud both the development and the deployment of their cyber capabilities in great secrecy.[26] States may also be reluctant to expose their vulnerabilities by discussing hostile cyber actions (and related damages), which were directed against them.[27]

A further explanation for the absence of state practice in applying IHL rules to cyberspace may relate, however, to a critical *legal* factor: the inherent difficulties in applying the IHL regime to information as a weapon and a target on the same basis that it is applied in conventional conflicts to physical forces, objects, and terrain. In this regard, assessing problems related to the origin, organization, and availability of information serves as a good starting point in illustrating the dimensions of information that complicate such a broad application of the IHL framework and the *jus ad bellum* to events in cyberspace.

1. Information: The Problem of Origin

Information, more so than physical objects and forces, may not permit those who are harmed by it to identify its origin or source. Computer specialists, engineers, scientists, and government experts

---

25. *See* Duncan B. Hollis, *An E-SOS for Cyberspace*, 52 HARV. INT'L L.J. 377, 404–05 (2011) ("No state has ever formally admitted its complicity in a cyberattack or cyberexploitation; nor is there any consensus on any state having done so in violation of international law.").

26. *See* JEFFREY HUNKER, CREEPING FAILURE: HOW WE BROKE THE INTERNET AND WHAT WE CAN DO TO FIX IT 92 (2010) (noting how "cyberwarfare competition is shrouded in secrecy, making it difficult to determine national vulnerabilities and threats").

27. For example, while Iran admitted that its computers at a nuclear facility had been infected by the so-called Stuxnet worm, it has at various times denied that the malware damaged any of the facility's systems. *See* Glenn Kessler, *Iran's Nuclear Program Reportedly Struggling*, WASH. POST (Nov. 22, 2010, 8:44 PM), http://www.washingtonpost.com/wp-dyn/content/article/2010/11/22/AR2010112206746.html (noting that, despite evidence to the contrary, "Iran denies the worm caused any problems"); *see also* Martin C. Libicki, *Sub Rosa Cyber War*, *in* THE VIRTUAL BATTLEFIELD: PERSPECTIVES ON CYBER WARFARE 53, 58 (C. Czossek & Kenneth Geers eds., 2009) (arguing that "[t]he overall motive – for both sides – for keeping matters out of the press is that cyber warfare is a negative-sum game").

continue to make well-funded efforts to develop better methods and "forensics" for identifying the physical source and ultimate origin of data packages used in hostile cyber actions.[28] In spite of these efforts, the nature of the information—and the nature of the Internet—makes it difficult, if not impossible, to identify the origin of information used as a weapon and the intent motivating those employing it.[29]

Because cyberspace is primarily a domain of information, it has only limited physical connections and properties (unlike the domains of land, sea, air, and space) and is characterized by many invisible actions.[30] Even if some malicious acts in cyberspace can be traced to specific physical connections, the ultimate origin of the harmful information may remain a mystery because of the nature of information. One impediment is that information in harmful computer programs can also be used to commandeer and remotely control other computers or computer networks.[31] These compromised computers ("zombies") or compromised networks ("botnets") may then direct or support a wide variety of malicious acts in cyberspace without the knowledge or consent of the users.[32]

Using the methods described above, hackers, criminals, and other actors routinely make use of hijacked systems and networks to engage in unauthorized cyber activities while avoiding detection and

---

28. *See, e.g.*, DOD CYBERSPACE POLICY REPORT, *supra* note 5, at 4 (discussing the DoD improvements in cyber forensics, including support for the Defense Cyber Crime Center).

29. Herbert Lin noted that

> [n]o one has come close to solving the problem of technical attribution – the ability to identify the party responsible for an offensive cyber operation based only on technical indicators and information associated with that operation. . . . [I]n the worst case, it may be difficult or impossible even to know when an offensive cyber operation has begun, who the attacker is, and what the operation's purpose and effects are or were.

See Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SEC. L. & POL'Y 63, 77 (2010).

30. *See* Libicki, *supra* note 27, at 55 (noting the possibility of "sub rosa" cyber attacks since "information systems are generally invisible" even if the artifacts of a system may be seen).

31. *See* John Markoff, *Attack of the Zombie Computers Is Growing Threat*, N.Y. TIMES (Jan. 7, 2007), http://www.nytimes.com/2007/01/07/technology/07net.html?pagewanted=all&_r=0 (noting that criminals are, "with growing sophistication . . . taking advantage of programs that secretly install themselves on thousands or even millions of personal computers, band these computers together into an unwitting army of zombies, and use the collective power of the dragooned network to commit Internet crimes").

32. *See id.* (noting that botnets "are being blamed for the huge spike in spam that bedeviled the Internet in recent months, as well as fraud and data theft" and that security researchers "have been concerned about botnets for some time because they automate and amplify the effects of viruses and other malicious programs").

concealing their identities.[33] In the case of hostile, state-sponsored actions, the difficulty in identifying the genuine origin of damaging information is only the first step in the arduous process of attributing the transmission of such information to a responsible state. Next comes the challenging task of establishing a legally sufficient connection between an actor—who may appear to be a private person, linked only to privately owned systems and networks—and a specific government.

Determining the origin of information used in a hostile cyber action, identifying its geographic contours, and attributing the transmission of that information to specific persons and then to a responsible state can thus be a Herculean task. This intractable problem is clearly reflected in the current practice of states. One important example of such state practice (or nonpractice) is found in what some have referred to as the first cyber attack by one country on another: the three-week wave of hostile cyber actions against government, media, and financial websites and other computer systems and networks in Estonia in 2007.[34]

While many observers alleged that the hostile cyber actions taken against Estonia in 2007 were directed or sponsored by the Russian government, the origin of these actions, their geographic nexus, and the identity of the responsible parties remain unknown.[35] Instead, investigators found only a shadowy world of "Russian hacktivists," "criminal botnets," and a trail that ultimately led them to computers located primarily in Western countries.[36] Similarly, notwithstanding unofficial accounts of persons in the United States allegedly participating in the deployment of the much-discussed "Stuxnet worm" (a sophisticated malware program that was apparently directed against Iranian nuclear facilities), the positive

---

33. *See* Nicole Perlroth, *Researchers Say They Took Down World's Third-Largest Botnet*, N.Y. TIMES BLOG (July 18, 2012, 6:25 PM), http://bits.blogs.nytimes.com/2012/07/18/cybersecurity-researchers-say-they-took-down-worlds-third-largest-botnet/ (noting that "[t]echnologists have taken the lead in combating digital crime rather than waiting for law enforcement authorities to act" and how computer security experts "took down . . . a cluster of infected computers used by cybercriminals . . . that was responsible for roughly . . . 18 billion spam messages a day").

34. *See* Peter Finn, *Cyber Assaults on Estonia Typify a New Battle Tactic*, WASH. POST, May, 19, 2007, at A1 (noting that Estonia "has been subject in recent weeks to massive and coordinated cyber attacks on Web sites of the government, banks, telecommunications companies, Internet service providers and news organizations").

35. *See* Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, THE GUARDIAN (May 16, 2007), http://www.theguardian.com/world/2007/may/17/topstories3.russia (stating that there is disagreement among experts as to whether the identity of the "cyber-warriors" can be established).

36. *Cyberwar: War in the Fifth Domain*, THE ECONOMIST, July 1, 2010, at 28; *see* Hollis, *supra* note 25, at 405 ("We still do not know who authored the 2007 Estonia attacks . . . .").

identification of responsible persons or governments has been a significant and elusive technical challenge.[37]

It is thus for good reason that one scholar argues that while "proponents of rules on cybercrime and cyberwar regularly assume that sufficient attribution of an attack's origins can and will occur. . . . In reality, however, anonymity, not attribution, prevails."[38] The strategic significance of this phenomenon and the threat that it presents to U.S. national interests has been duly noted by the DoD.[39] While it may be tempting to dismiss attribution in cyberspace as a mere technical problem waiting to be overcome, the unique properties of information and the architecture of the Internet itself ensure that this is a systemic problem.[40]

The fundamental origin and attribution problems discussed above cast long shadows over the application of IHL rules in cyberspace and also over international law governing the right of states to use armed force in response to perceived cyber attacks. As expressed in Article 51 of the UN Charter, the *jus ad bellum* limits the right of states to use armed force in self-defense to those situations in which an "armed attack" occurs.[41] This right to use armed force in self-defense is also dependent on meeting a high threshold for attribution of the armed attack.[42]

As discussed below, extraordinary difficulties in attributing the information used in hostile cyber actions appear to significantly impede efforts to characterize such actions as armed attacks justifying the use of armed force in self-defense under the UN Charter. As the world advances further and further into an apparent age of cyber conflict, the continuing failure of states to treat damaging cyber acts standing alone as armed attacks is highly

---

37. *See The Stuxnet Outbreak: A Worm in the Centrifuge*, THE ECONOMIST, Sept. 30, 2010, at 63 (noting that "America and Israel are the obvious suspects. But Stuxnet's origins and effects are unknown."); David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1 (noting that while forensic investigations into the inner workings of the Stuxnet "were successful in picking apart how the code worked," those investigations "came to no conclusions about who was responsible").

38. Hollis, *supra* note 25, at 377–78.

39. *See* DOD CYBERSPACE POLICY REPORT, *supra* note 5, at 4 (noting that "[o]ur potential adversaries, both nations and non-state actors, clearly understand this dynamic and seek to use the challenge of attribution to their strategic advantage").

40. Hollis, *supra* note 25, at 397 ("Those with sufficient technical skill can remain anonymous at will. . . . This situation is unlikely to change anytime soon; it is a systemic aspect of the Internet, not a simple problem to be fixed.").

41. U.N. Charter art. 51 ("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.").

42. *See, e.g.*, Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161 (Nov. 6) ("[I]n order to establish that it was legally justified in attacking the Iranian platforms in exercise of the right of individual self-defence, the United States has to show that attacks had been made upon it for which Iran was responsible.").

significant since the establishment of customary international law is dependent on the finding of such state practice (done out of a sense of legal obligation, or *opinio juris*).[43]

Notwithstanding the notable absence of supporting state practice to this point in history, some authors suggest new norms that treat destructive cyber operations as unlawful uses of force can be expected to emerge.[44] However, drawing on extant (as opposed to desired) state practice, one might also argue that the problematic characteristics of information as a weapon and target are contributing to a reluctance by states to embrace such a norm.

States have in fact to this point refrained from invoking the right to self-defense in response to hostile cyber acts alone, even though destructive cyber programs have been employed by states for many decades. For example, in 1982 an early version of a "logic bomb" (reportedly planted by the Central Intelligence Agency in a computer-control system stolen by Soviet spies from a Canadian firm) caused a malfunction in a Soviet gas pipeline in Siberia, resulting in a massive explosion.[45] States have also had access to harmful viruses and other malicious computer programs since the early years of the Internet itself.[46]

There is, however, no shortage of rhetoric from government officials and military leaders warning that hypothetical, highly destructive cyber acts in the future will be regarded as conventional armed attacks and armed force will be used in response.[47] States are understandably unwilling to officially foreclose their right to use all necessary means to respond to any serious threat, including the most destructive cyber acts.[48] However, to this point, no state has used armed forced against another state nor actually invoked its right to

---

43. *See* Continental Shelf (Libya v. Malta), 1985 I.C.J. 29, ¶ 27 (June 3) ("It is of course axiomatic that the material of customary international law is to be looked for primarily in the actual practice and *opinio juris* of States.").

44. *See, e.g.*, Michael Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 VILL. L. REV. 569, 588 (2012) (noting that "[i]n light of the increasing frequency and severity of cyber operations, a tendency towards resolving grey areas in favor of finding a use of force can be expected to emerge").

45. *See Cyberwar: War in the Fifth Domain*, *supra* note 36, at 25 (quoting the memoirs of Thomas Reed, a former Air Force secretary, that the result of this logic bomb "was the most monumental non-nuclear explosion and fire ever seen from space").

46. *See* Markoff, *supra* note 31 (noting how "[p]lagues of viruses and other malicious programs have periodically swept through the Internet since 1988, when there were only 60,000 computers online").

47. *See, e.g.*, Gorman, *supra* note 7 (quoting a U.S. military official as saying, "If you shut down our power grid, maybe we will put a missile down one of your smokestacks").

48. *See, e.g.*, THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE 14 (May 2011) ("We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.").

do so in response to hostile cyber actions alone; nor has any state claimed before the UN Security Council that hostile cyber actions alone have made that state the victim of an armed attack and reported actions taken pursuant to its right of self-defense (as required by the UN Charter).[49]

Significantly, the much-discussed cyber actions taken against Estonia in 2007 only reinforced this absence of state practice, since Estonia never officially claimed to be the victim of an armed attack before the UN Security Council and never invoked its right to self-defense under Article 51. Instead, Estonia acknowledged great difficulties in attributing responsibility for the attacks and generally treated the incident as the work of criminal organizations.[50] Rather than attributing the actions to a foreign government, an Estonian government official would later describe the event as "a mass cyber riot."[51]

Any cyberwar narrative for the incidents that occurred in Estonia in 2007 is also fundamentally at odds with the official statements of both the Estonian Ministry of Defense and NATO officials.[52] Furthermore, the Estonian minister of defense candidly noted that "[n]ot a single Nato defence minister would define a cyber-attack as a clear military action at present."[53] Such current state practice stands in stark contrast to alternate scenarios suggested by some authors, in which states that suffer "massive cyber attacks, similar to or more aggravated than those suffered by Estonia, may choose to treat them as justifying a forceful response."[54]

In spite of the reality of current state practice, which rejects equating hostile cyber acts with illegal uses of force, there is no shortage of commentators, government officials, and former

---

49. UN Charter art. 51.

50. *See* C. CZOSSECK & K. GEERS, THE VIRTUAL BATTLEFIELD: PERSPECTIVES ON CYBER WARFARE 186–87 (2009) (noting that cyber "attacks" on Estonia "resulted in the arrest and successful prosecution of one Estonian citizen" and that the Estonian chief prosecutor declared that "[w]e have no evidence and no information that this was the Russian government").

51. *See* Andy Greenberg, *When Cyber Terrorism Becomes State Censorship*, FORBES (May 14, 2008, 6:00 PM), http://www.forbes.com/2008/05/14/cyberattacks-terrorism-estonia-tech-security08-cx_ag_0514attacks.html (further noting that the Estonian director of eGovernance specifically "discounted theories about the involvement of the Russian government").

52. *See* Traynor, *supra* note 35 (quoting the Estonian defense minister as saying that "[a]t present, Nato does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country.").

53. *Id.*

54. *See* Schmitt, *supra* note 44, at 588 (further stating that "[i]f state practice along these lines became widespread and well-accepted, the Article 51 norm would shift accordingly through the natural process by which existing international law remains current. For the moment, that has not occurred.").

government officials (especially those who are now associated with cyber security firms) offering sensationalized accounts of current or imminent so-called cyberwars.[55] The word *war* in the context of cyberspace has thus become more of a political or cultural term than a legal one (joining "wars" against poverty, crime, drugs, and obesity), with little relevance to the legal right of states to use armed force in response to hostile cyber acts.

Setting aside sensationalized war rhetoric, the fundamental problem of identifying the origin of information used in hostile cyber acts continues to make it extremely difficult for states to equate such acts with armed attacks justifying armed responses. The anonymity of information and the structure of the Internet are more than simply "factors" to be used in evaluating the legal status of hostile cyber acts. Instead, origin and attribution problems have dominated all major cases reported to date, impeding any effort to apply the *jus ad bellum* regime to hostilities in cyberspace.[56] These problems continue to figure prominently in making contemporary reports of cyber attacks phantoms under the *jus ad bellum*.

Systemic problems in identifying and legally attributing the origins of information also fundamentally impair the meaningful application of the *jus in bello*—that is, the IHL framework—to conflicts in cyberspace. A conclusion that the IHL framework governs particular events in cyberspace determines numerous issues, including whether the domestic law enforcement model is displaced in favor of the armed conflict model and whether key IHL rules apply.[57]

The most important IHL obligations include requirements that: (1) attacks must never be directed against civilian objects and must always distinguish between civilian and military objectives (the principles of discrimination and distinction); (2) attacks must not cause injury or damage to civilian objects in excess of the concrete and direct military advantage to be gained even when directed against legitimate military objectives (the principle of proportionality); and (3) those persons responsible for planning and

---

55. *See* Evgeny Morozov, *Battling the Cyber Warmongers*, WALL ST. J., May 8–9, 2010, at W3, col. 1 (condemning "cyber-jingoism from former and current national security officials," including those now associated with security firms who may have a vested interest in exaggerating cyber threats).

56. For example, the origin of the "attacks" against Estonia was traced to at least 177 countries other than Estonia. *See* Charles Clover, *Kremlin-Backed Group Behind Estonia Cyber Blitz*, FIN. TIMES (Mar. 11, 2009, 2:00 AM), http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz2jcIdHjuX.

57. *See generally* GARY D. SOLIS, THE LAW OF ARMED CONFLICT 164–86 (2010) (contrasting, in the context of terrorism, the "criminal justice model" characterized by the traditional investigation of crimes and the arrest and trial of individuals for violations of domestic law with the "military model" characterized by very different detention practices, the permissive use of force, the application of the law of armed conflict, and a focus on military objectives rather than on "justice").

carrying out attacks must take all feasible precautions to ensure adherence to the principles of distinction and proportionality ("precautionary measures").[58]

Both states and individuals are responsible for their conduct under the IHL framework.[59] However, a state is only responsible for IHL violations that can be legally attributed to that state. While attribution may be a relatively routine matter in the context of many conventional armed conflicts, the nature of information makes attribution highly problematic for conflicts in cyberspace. In fact, it has been suggested that this problem of attribution is perhaps the most fundamental and serious challenge to the application of the IHL framework to conflicts in cyberspace, as well as efforts to regulate cybercrime.[60]

2. Information: The Problems of Organization and Armed Conflict Classification

While attribution of responsibility for hostile cyber actions to states is dominated by the problem of identifying the origin of those actions, it can also be greatly affected by problems related to the way persons can use information to anonymously organize themselves in cyberspace. The absence of physical controls and the possibilities of virtual organization may present significant obstacles to making the legal determinations necessary to attribute cyber conduct by individuals to states.

The establishment of an armed conflict and the classification of that conflict are both critical threshold determinations for applying the IHL framework.[61] These determinations may in turn depend on the establishment of various degrees of organization and control of the actors. While making such determinations may at times present

---

58. Protocol I, *supra* note 22, at arts. 51, 52, 57. These provisions reflect customary international humanitarian law related to "precautions in attack." *See* JEAN-MARIE HENCKAERTS & LOUIS DOSWALD-BECK, I CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 51–67 (2005).

59. While states are clearly bound by the international legal obligations found in treaties to which they are a party and by applicable rules of customary international law, it is important to also note that the principle of *individual* responsibility (and punishment) for crimes under international law (including the IHL framework) has been described as the "cornerstone of international criminal law" and is the enduring legacy of the Nuremberg Tribunals. Prosecutor v. Tadic, Case No. IT-94-1-I, Opinion and Judgment, ¶ 665 (Int'l Crim. Trib. for the Former Yugoslavia May 7, 1997) (internal citations omitted).

60. *See* Hollis, *supra* note 25, at 378 ("[A]nonymity makes it difficult—if not impossible—for rules on either cybercrime or cyberwar to regulate or deter.").

61. *See* Kenneth Watkin, *Chemical Agents and "Expanding" Bullets: Limited Law Enforcement Exceptions or Unwanted Handcuffs?*, 82 J. INT'L LEGAL STUD. 193, 199 (2006) ("The application of the law of war is dependent upon the categorization of conflict. . . . [T]he establishment of law and order is ultimately dependent on the drawing of jurisdictional lines.").

vexing questions in the physical world, efforts to establish necessary levels of organization and control in cyberspace confront even more serious challenges.

In order for the IHL framework to apply, either an "international armed conflict" or "noninternational armed conflict" is required. The Geneva Conventions of 1949 provide that an international armed conflict is present in "all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties."[62] As further explained in the *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (*Commentary*), the official International Committee of the Red Cross (ICRC) commentary on Common Article 2 of the Geneva Conventions, "[A]ny difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2 . . . ."[63]

Because it focuses primarily on the actions of members of the armed forces of states, the legal framework for attribution of responsibility for IHL violations in conventional international armed conflicts may be relatively uncomplicated. For example, it is not controversial that responsibility for IHL violations can be attributed to states based on the conduct of its military personnel.[64]

In theory, then, if hostile cyber acts can be linked to the military personnel of a state in an international armed conflict, related IHL violations can be attributed to that state. That link may, of course, be difficult to actually establish in light of the inherent difficulties associated with identifying the origins of information in cyberspace. Furthermore, establishing state control over other types of actors—based on information residing in or passing through cyberspace—may be even more difficult, significantly impeding the attribution of IHL violations by those actors to a state.

In addition to state responsibility based on the conduct of its military personnel, customary international law provides that a state is also responsible for violations of IHL obligations by other persons under various circumstances. These circumstances include violations attributed to a state that are committed by "persons or entities it

---

62. Geneva Convention Relative to the Treatment of Prisoners of War art. 2, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 (This article is found in all four 1949 Geneva Conventions and thus is referred to as Common Article 2).

63. INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE GENEVA CONVENTIONS OF AUGUST 1949: III GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR art. 2, ¶ 1 (Jean S. Pictet ed., 1960) (internal footnote omitted); *see also* INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 ¶ 62 (Yves Sandoz, Christophe Swinkarsi & Bruno Zimmermann eds., 1987) [hereinafter COMMENTARY ON THE ADDITIONAL PROTOCOLS] ("[H]umanitarian law . . . covers any dispute between two States involving the use of their armed forces.").

64. *See* Protocol I, *supra* note 22, at art. 91 (providing that a party "shall be responsible for all acts committed by persons forming part of its armed forces").

empowered to exercise elements of governmental authority," by "persons or groups acting in fact on its instructions, or under its direction or control," or by "private persons or groups which it acknowledges and [whose conduct it] adopts as its own."[65]

While the International Court of Justice (ICJ) has acknowledged that conduct by private persons or groups acting under the direction or control of a state can be attributed to that state for purposes of IHL violations, it has also established a very high standard for such attribution. In *Nicaragua v. United States*, the court concluded that for the United States to be held responsible for alleged IHL violations committed by "Contra" paramilitaries operating in Nicaragua, it would have to be established that the United States had "effective control over the military or paramilitary operations in the course of which the . . . violations [occurred]."[66]

The International Criminal Tribunal for the Former Yugoslavia (ICTY) has indicated that for some purposes, including establishing individual criminal responsibility, "the extent of requisite State control varies."[67] Nonetheless, the ICJ has not abandoned the high "effective control" threshold it established in the *Nicaragua* case for attribution of conduct to states.[68]

As demonstrated by the *Nicaragua* case and subsequent ICJ decisions, sufficient state control for attribution purposes may be difficult to establish in armed conflicts in the physical world in spite of the availability of physical evidence and the significance of a state's responsibility for conduct occurring on its own territory. With the links between states and persons so difficult to establish in cyberspace, proving effective state control over persons and groups in cyberspace presents an even more daunting challenge.

The ability of individuals to use information to form loosely affiliated cyber "groups" that collectively engage in destructive actions presents a final, significant classification problem under the IHL framework. Common Article 3 to the Geneva Conventions establishes a second category of armed conflicts, referring to them only as those "not of an international character occurring in the

---

65. HENCKAERTS & DOSWALD-BECK, *supra* note 58, rule 149, at 530.

66. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 115 (June 27).

67. Prosecutor v. Tadic, Case No. IT-94-1-A, Judgment, ¶¶ 120, 137 (Int'l Trib. for the Former Yugoslavia July 15, 1999) ("[F]or the attribution to a State of acts of these groups it is sufficient to require that the group as a whole be under the overall control of the State.").

68. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, 226, ¶ 60 (Dec. 19) (stating that it could not conclude that the conduct of the Movement for the Liberation of Congo was "on the instructions of, or under the direction or control of' Uganda," thus not revisiting the question of "whether the requisite tests [as set forth in the Nicaragua case] are met for sufficiency of control of paramilitaries").

territory of one of the High Contracting Parties."[69] According to the ICTY, these noninternational conflicts are characterized by "protracted armed violence between governmental authorities and organized armed groups or between such groups within a State."[70]

The requirement that noninternational armed conflicts reach a particular level of intensity and involve the participation of organized armed groups is well established.[71] Such conflicts are to be contrasted with other forms of violence to which the IHL framework does not apply—namely, "situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature."[72] The phrase "situations of internal disturbances and tensions" encompasses an extremely diverse set of acts that are generally governed by the domestic criminal law of states. Such disturbances and tensions could include many harmful actions of individuals and groups operating in both physical domains and cyberspace.

Through the use of information and the Internet, it is possible for members of a decentralized online community, acting anonymously, to engage in loosely coordinated, destructive actions—sometimes in support of a particular government's interests (although their connection with that government may be unclear or impossible to establish).[73] These cyber communities can take advantage of the ability of individual actors in cyberspace to use information to coordinate damaging actions without a leadership structure, physical interaction, or command and control systems. For example, one such notorious "organization" known as Anonymous, which uses an image

---

69. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 3, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31.

70. Prosecutor v. Tadic, Case No. IT-94-1-AR72, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995); *see also* Prosecutor v. Akayesu, Case No. ICTR-96-4-T, Judgment, ¶ 619 (Int'l Crim. Trib. for Rwanda Sept. 2, 1998) (citing this finding in *Tadic*).

71. Sylvain Vite, *Typology of Armed Conflicts in International Humanitarian Law: Legal Concepts and Actual Situations*, 91 INT'L REV. OF THE RED CROSS 69, 76 (2009).

72. *Id.* (internal citation omitted); *see also* Rome Statute of the International Criminal Court art. 8(2)(f), July 17, 1998, 2187 U.N.T.S. 90 (distinguishing various situations of internal disturbances and tensions from armed conflicts not of an international character); Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment (Trial Chamber), ¶ 84 (Int'l Trib. for the Former Yugoslavia Nov. 30, 2005) (distinguishing an armed conflict "from banditry, unorganized and short-lived insurrections, or terrorist activities, which are not subject to international humanitarian law") (internal citation omitted).

73. *See, e.g.*, Michael Moynihan, *You're Being Hacked; Cyberspies are Everywhere. But Who are They Helping?*, NEWSWEEK, May 29, 2013, at 1 (describing the diverse, harmful cyber activities of various anonymous hacker collectives, including one that calls itself "the Syrian Electronic Army" that supports Syrian President Bashar al-Assad).

of a suit without a head to represent its leaderless, anonymous status, has been described as a loose "hacking collective." [74]

The structural organization that characterizes an armed force in conventional military operations involves varied elements of physical command and control and discipline, allowing physical violence to be organized and effectively directed against targets. Regardless of the damage that cyber communities or collectives may cause, their structurally limited, purely information-based coordination capabilities and their inability to engage in protracted armed violence make them highly unlikely to meet the thresholds for organization and intensity required for armed groups in noninternational armed conflicts.

To the extent that the IHL regime may require armed groups to be sufficiently organized to impose discipline, engage in sustained military operations, and exercise physical control over persons or territory, the limitations of cyber groups further highlight the legal significance of the distinction between physical and informational organization. [75] It is thus not surprising that even writers who emphasize the importance of the damaging consequences of cyber actions conclude that "[i]t would be exceptionally difficult for cyber operations standing alone to rise to the level of noninternational armed conflict."[76]

3. Information: The Problem of Territory

In denying Russian responsibility for cyber actions that allegedly emanated from Russian territory and damaged Estonian computer systems and networks, the Russian ambassador to the European Union famously remarked that "cyberspace is everywhere."[77] Such comments reflect the reality that the nonterritorial dimensions of information in cyberspace pose serious challenges to establishing a state's responsibility for actions on the basis that those actions "originated from," "occurred," or "took place" on its territory.

Conventional legal concepts of responsibility based on physical terrain and control of territory are fundamentally impaired by the

---

74. Nicole Perlroth, *Hackers Interrupt Service at the C.I.A.'s Web Site*, N.Y. TIMES, Feb. 11, 2012, at B2.

75. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 1, June 8, 1997, 1125 U.N.T.S. 609 [hereinafter Protocol II] (applying a higher threshold than Common Article 3 by referring to "organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol").

76. Michael Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 151, 176 (2010) [hereinafter CYBERATTACK WORKSHOP PROCEEDINGS].

77. Traynor, *supra* note 35.

realities of cyberspace. Even if information used in a hostile cyber action may eventually be traced to physical connections or nodes on the territory of one state, many of the systems or networks involved may be remotely controlled, as previously noted, by information originating from the territory of another state. Finding a "responsible" computer or network under these circumstances is unlikely to implicate either individual or territorial state responsibility since the hostile actions in question may have been unauthorized or even unknown by the owner of the computer systems or networks in question. [78] Furthermore, attribution of state responsibility may be significantly impeded by the lack of government control or even presence in cyberspace. Unlike other physical domains, much of cyberspace is privately owned.[79]

Private ownership of much of cyberspace creates complex relationships between states and private actors that cloud state responsibility for actions involving the misuse of information at the physical connections or terminals located on its territory.[80] These relationships are further muddled by individual states' different regulatory and legal systems governing the use of the Internet (including restrictions on content and expression), access to privately owned information systems, privacy rights, and the information itself.[81]

While the links that connect information with territory, states, and nonstate actors may be exceedingly tenuous or impossible to find, some commentators have nonetheless argued that states should be held responsible under various circumstances for "cyber attacks . . . continuously launched from within [their] borders."[82] Assuming (with difficulty) that the country of origin of a hostile cyber act can be

---

78. *See* MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 3–4 (2009) ("[M]illions, perhaps tens of millions, of computers today are bots, capable of being controlled by nefarious others their owners have never met.").

79. *See* U.S. DEP'T OF DEF., STRATEGY FOR OPERATING IN CYBERSPACE 5 (2011) [hereinafter DOD CYBERSPACE STRATEGY] ("[T]he networks and systems that make up cyberspace are man-made, often privately owned, and primarily civilian in use . . . .").

80. *See id.* at 8 ("The challenges of cyberspace cross sectors, industries, and U.S. government departments and agencies; they extend across national boundaries and through multiple components of the global economy. Many of DoD's critical functions and operations rely on commercial assets, including Internet Service Providers (ISPs) and global supply chains, over which DoD has no direct authority to mitigate risk effectively.").

81. The lack of international consensus in efforts to regulate cyberspace illustrates these complex relationships. *See* Viktor Mayer-Schönberger, *The Shape of Governance: Analyzing the World of Internet Regulation*, 43 VA. J. INT'L L. 605, 627–28 (2003) ("Any attempt to harmonize cyber-regulation on a global scale and by consensus would have to overcome supreme hurdles . . . ."); *Private Data, Public Rules*, THE ECONOMIST, Jan. 28, 2012, at 59 (noting that although states are making plans to govern internet markets to protect privacy, "their approaches differ wildly").

82. *E.g.*, David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 94–95 (2010).

identified, these theories posit that a state should be held responsible for such acts if it serves as a "sanctuary" for nonstate actors engaging in cyber attacks—as determined by that state's failure to enact and enforce on its territory stringent criminal laws against such attacks, to appropriately investigate them, and to fully cooperate with other states in efforts to identify, apprehend, and punish those who engage in these attacks.[83]

As a general matter, and particularly with respect to *jus ad bellum* issues, state responsibility for actions—even physical ones—that occur on its territory may often be overstated. At the outset, the state's knowledge of such actions may not always be presumed.[84] In addition, even in the physical world, responsibility for those actions must still be imputed to the authorities of that state.[85] In cyberspace this is of course highly problematic, especially since "[n]o method exists of determining whether the individual at the other end of the attacks is a government agent."[86]

With respect to the legal standard governing state responsibility for the actions of groups operating on its territory, it has been suggested that a new threshold, lower than the effective control standard articulated in *Nicaragua*, has emerged as a result of the actions taken against the Taliban regime in Afghanistan in response to the 9/11 attacks.[87] As previously noted, however, a lower threshold cannot be found in ICJ decisions, nor is it clearly reflected in state practice, notwithstanding the exceptional circumstances surrounding the intervention by NATO in Afghanistan in 2001.

---

83. *See id.* at 93–94 (assessing violations of state duties to prevent cyber attacks).

84. The court found that

> [i]t cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or ought to have known, the authors. This fact, by itself and apart from other circumstances, neither involves prima facie responsibility nor shifts the burden of proof.

See Corfu Channel (U.K. v. Albania), 1949 I.C.J. 18 (April 9).

85. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶155 (June 27) ("[E]ven supposing it well established that military aid is reaching the armed opposition in El Salvador from the territory of Nicaragua, it still remains to be proved that this aid is imputable to the authorities of the latter country.").

86. Eric Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, STAN. J. INT'L L. 207, 234 (2002).

87. *See* Graham, *supra* note 82, at 96 (discussing arguments for increasing state responsibility for actions of nonstate actors); *see generally* TAL BECKER, TERRORISM AND THE STATE: RETHINKING THE RULES OF STATE RESPONSIBILITY 212–38 (2006) (reviewing arguments for and against Taliban responsibility for Al Qaeda's actions on 9/11).

The extraordinarily close relationship between Al Qaeda and the Taliban regime resulted in a series of unprecedented sanctions by the UN Security Council against the Taliban regime (prior to the 9/11 attacks) for its widely recognized, direct, and continuing support of Al Qaeda, its leaders, and its terrorist activities. [88] These unique circumstances make NATO's post-9/11 actions against the Taliban regime a poor precedent upon which to build a case for a lowering of the effective control threshold or for creating a new "sanctuary" theory of state responsibility for the actions of groups in the physical world, let alone for the actions of groups in cyberspace.

Sanctuary theories of state responsibility for cyber attacks (based on a state's failure to enact and enforce on its territory stringent criminal laws against harmful cyber actions) may appear attractive, but they are not part of any obligations now expressed in international conventions or customary international law. To the extent any international consensus in this area can be said to be developing, a representative, nonbinding UN General Assembly resolution calls upon states to "ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies." [89] Unfortunately, this resolution refers neither to "attacks" nor to IHL obligations.

Furthermore, even in areas of criminal activity that the resolution is intended to address, its broad provisions have not yet been implemented in any manner indicating consistent, widespread, and conforming state practice. Instead, there continues to be a lack of international consensus regarding some of the most fundamental aspects of dealing with cybercrime and the misuse of information in cyberspace.[90]

There currently is only one significant, binding, multilateral agreement on the subject of cybercrime—the Council of Europe Convention on Cybercrime (CEC).[91] The CEC may be an important

---

88. *See* Jack M. Beard, *Military Action Against Terrorists Under International Law: America's New War on Terror: The Case for Self-Defense Under International Law*, 25 HARV. J.L. & PUB. POL'Y 559, 582–83 (2002) (also noting the unique evidentiary standards the United States employed in making its case for an armed response against the Taliban).

89. G.A. Res. 55/63, ¶ 1(a), U.N. Doc. A/RES/55/63 (Jan. 22, 2001); *see also* G.A. Res. 45/121, ¶ 3, U.N. Doc. A/RES/45/121 (Dec. 14, 1990).

90. *See* David Satola & Henry L. Judy, *Electronic Commerce Law: Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum*, 37 WM. MITCHELL L. REV. 1745, 1772 (2011) (noting how delegates at the Twelfth UN Crime Congress, held in April 2010 in Salvador, Brazil, were unsuccessful in negotiating a new global cybercrime treaty because issues there presented countries with "inherently conflicting policy objectives and cultural clashes, including the need to balance different interests and rights such as security and privacy").

91. Convention on Cybercrime, Council of Europe, Nov. 23, 2001, 41 I.L.M. 282, 2296 U.N.T.S. 167 (ratified by the United States in 2006, entered into force in 2007).

first step in protecting society from cybercrime by seeking to "harmonize national laws on cybercrime, improve national capabilities for investigating such crimes, and increase cooperation on investigations."[92] However, to date, only a modest number of states (mostly European ones) are parties to the CEC, and those states are also all able to take reservations in nine key designated areas.[93] Furthermore, the CEC does not address state sponsorship or support of harmful cyber activities (including espionage and cyber attacks) or state responsibility for actions under either the *jus in bello* or *jus ad bellum*.[94]

Rather than establishing a new norm of customary international law regarding state territorial responsibility for cyber attacks, state practice in this area instead reflects conscious neglect, confusion, lack of consensus, and enormous practical and legal difficulties in both determining the origin of hostile cyber actions and in imposing a territorial model on them. The current shadowy world of cybercrime and the related—and often indistinguishable—world of state-sponsored espionage and sabotage thrive on the lack of territorial boundaries in cyberspace, the invisible nature of information, and the lack of coordination and cooperation between states on cyber issues.

Varied types of hackers, hacktivists, and state-sponsored actors engage in diverse acts of mischief, crime, and destruction in cyberspace on a daily basis.[95] Most of these actors operate with impunity and successfully evade or manipulate the territorial boundaries of the states in which they operate, as demonstrated by the incredible lack of accountability for cyber threats under domestic legal regimes.[96] This profound inability of states to impose their own domestic criminal laws on cyber events that "occur" within their territories vividly illustrates the fragile nature of state territorial

---

92. Michael A. Vatis, *The Council of Europe Convention on Cybercrime, in* CYBERATTACK WORKSHOP PROCEEDINGS, *supra* note 76, at 207 (internal citation omitted).

93. States Party are permitted to make reservations in nine areas under Article 42. Convention on Cybercrime, *supra* note 91, at art. 42. As of December 31, 2013, 41 states were parties to the Convention. *See Convention on Cybercrime*, COUNCIL OF EUROPE, http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185& CL=ENG (last updated Jan. 5, 2014).

94. *See* Vatis, *supra* note 92, at 220 ("Moreover, the Convention does not address the particular concerns that may be raised by cyber attacks that are not just criminal acts, but may also constitute espionage or the use of force under the laws of war.").

95. *See The Nomination of John O. Brennan to be Director of the Central Intelligence Agency: Hearing Before the S. Select Comm. on Select Intelligence*, 113th Cong. (2013) (statement of John O. Brennan, Nominee, Director of the Central Intelligence Agency) ("U.S. computer networks and databases are under daily cyber attack by nation states, international criminal organizations, subnational groups, and individual hackers.").

96. *See* Hollis, *supra* note 25, at 404 ("[L]egal accountability for cyberthreats is exceedingly rare. At most, five percent of cybercriminals are arrested or convicted.").

control and responsibility over hostile uses of information in cyberspace and should caution against the summary application of international law on this basis.

It is true that a state may have an obligation to exercise "due diligence" in order to prevent conduct contrary to international law within its territory and to prosecute and punish such conduct if it occurs.[97] However, the absence of agreed legal obligations with respect to hostile cyber actions, the pervasive use of commandeered computer systems and networks, the transnational dimensions of information in cyberspace, and the widespread involvement of private entities and private property all work to impede clear findings of state responsibility with respect to the transmission of damaging information.

4. Information: The Problems of Unlimited Availability and Ubiquitous Processors

As noted above, the predominance of privately owned assets in cyberspace and the widespread availability of information and sophisticated information technologies give rise to unparalleled asymmetric warfare capabilities. Because of the exceedingly low barriers to entry in the arena of information (anyone can create it) and the acquisition of information technology (almost anyone can buy it), even the most powerful states are facing serious cyber threats from an unprecedented number of new actors.[98] In fact, states are already being subjected, on a daily basis, to costly intrusions by adversaries with increasingly sophisticated cyber capabilities.[99]

While state actors are generally responsible for the operation of various sophisticated weapon systems and armaments such as tanks, ballistic missiles, and warships, those who possess information and who operate potentially harmful information technologies operate in a new sort of "weapons commons." Nonstate actors, notably transnational terrorist organizations, have long known the value of the Internet as a means of financing and publicizing terrorist activities and recruiting new members—making information technologies and interconnectedness key aspects of modern

---

97. *See* Marco Sassòli, *State Responsibility for Violations of International Humanitarian Law*, 84 INT'L REV. OF THE RED CROSS 401, 411–12 (2002) (discussing state responsibility for violations of IHL obligations based on lack of due diligence).

98. *See* Lynn, *supra* note 17, at 98–99 ("A dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States' global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target.").

99. *See* DOD CYBERSPACE STRATEGY, *supra* note 79, at 3 ("Foreign cyberspace operations against U.S. public and private sector systems are increasing in number and sophistication. DoD networks are probed millions of times every day, and successful penetrations have led to the loss of thousands of files from U.S. networks and those of U.S. allies and industry partners.").

insurgencies. [100] Now a variety of cyber tools and methods, representing a new set of asymmetric warfare capabilities, are also available to these groups as potential weapons to inflict damage on their enemies.

A powerful addition to the cyber capabilities of nonstate actors may ironically come from the arsenals of the most technologically advanced states. Soon after powerful states use their most sophisticated cyber weapons, the information necessary to recreate these weapons may be readily available for downloading from the Internet. This phenomenon, which is said to be illustrated by information now available about the Stuxnet worm, has led some commentators to observe that the most sophisticated state-developed cyber capabilities may quickly become "open source" weapons once they are used.[101]

These developments mean that states now confront a vast array of new methods and means of warfare, a host of new cyber actors, and an abundance of new places from which hostile cyber actions against them can be taken. This reality of so many easily armed, diverse, and dangerous actors fundamentally complicates the task of determining the origin of specific hostile actions.[102] While many physical weapons may be distributed widely among nonstate actors, such weapons have physical properties and present physical evidence of their possession and use; such evidence is not present in the transmission of various types of information through cyberspace.

The abundance of actors in cyberspace and the widespread availability of new information weapons also raise difficult questions about the IHL status of the many persons who design and create computer programs, use the computer systems and networks, or contribute in other ways to processing or managing information packages that may be used in hostile cyber acts. Under IHL rules, civilians enjoy a protected status and are immune from attack unless they take a "direct" or "active" part in hostilities.[103] The dawn of a new era of abundant information weapons presents the unsettling possibility of an expanded and ambiguous type of involvement by the civilian population in armed conflicts.

---

100. *See* U.S. ARMY, U.S. MARINE CORPS, COUNTERINSURGENCY FIELD MANUAL NO. 3-24, ch. 1, ¶ 22 (Dec. 2006) ("Using the Internet, insurgents can now link virtually with allied groups throughout a state, a region, and even the entire world.").

101. *See* Evan Pickworth, *Bank Cyber Fraud More Lucrative Than Drugs Trade*, MAIL & GUARDIAN (Aug. 16, 2011) (noting the "major risk" in "the growth in usage of open source weapons like the Stuxnet virus that is freely available online for download").

102. *See* DOD CYBERSPACE POLICY REPORT, *supra* note 5, at 8 ("The often low cost of developing malicious code and the high number and variety of actors in cyberspace make the discovery and tracking of malicious cyber tools difficult.").

103. *See International Humanitarian Law*, *supra* note 10, at 734 ("The notion of 'direct' or 'active' participation in hostilities, which is derived from Article 3 common to the Geneva Conventions, is found in multiple provisions of IHL.").

The question of what constitutes "direct participation in hostilities" already raises difficult issues in conventional armed conflicts.[104] In light of the diverse types of actions that can be performed by individuals as they create, process, or otherwise use abundant information resources—from designing malware to managing websites or simply processing data—questions of civilian immunity under the IHL framework become even more complex.

The many interrelated activities that may be involved in the processing or management of information related to a particular hostile cyber action will also raise difficult questions about the specific conditions under which civilians involved in these activities could lose their immunity from direct attack. If, for example, civilians are immune from direct attack "unless and for such time as they take a direct part in hostilities,"[105] defining the precise temporal period of an individual's work on a computer during which he or she could be legally susceptible to attack may present some serious challenges.

Difficulties in determining the status of individuals engaged in cyber activities in the context of noninternational armed conflicts present further challenges. In order to distinguish civilians in these conflicts from members of insurgencies and other organized armed groups of nonstate actors, the ICRC takes a functional approach by suggesting that such armed groups "consist only of individuals whose continuous function it is to take a direct part in hostilities ('continuous combat function')."[106] Thus, if the IHL regime is extended to encompass cyber activities in these conflicts, this approach will likely raise problematic questions about the status of persons who, by continuously engaging in various damaging, diverse, and interrelated information and computer activities (including the preparation, execution, or command of such activities), are said to assume a continuous combat function that amounts to direct participation in hostilities.

---

104. In spite of the serious legal consequences that are attached to the phrase "direct participation in hostilities," no definition of the conduct by civilians that would render them subject to attack under this standard is found in the Geneva Conventions or their Additional Protocols.

105. Protocol I, *supra* note 22, at art. 51(3). This standard, suggesting only a temporal loss of protection, has not achieved universal acceptance. The United States, for example, is not a party to Protocol I, and its military regulations provide only that noncombatants may not be deliberately attacked, "unless they forgo their protection by taking a direct part in hostilities." DEP'T OF THE NAVY & DEP'T OF HOMELAND SEC., COMMANDERS HANDBOOK ON THE LAW OF NAVAL OPERATIONS, NWP 1-14M, ¶ 8.2.4 (July 2007).

106. NILS MELZER, INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 27, 34 (2009) (further noting that "individuals whose continuous function involves the preparation, execution, or command of acts or operations amounting to direct participation in hostilities are assuming a continuous combat function").

Specific and widely acknowledged examples of direct participation in hostilities by civilians in information-related cyber actions are difficult to find. The ICRC broadly identifies "interfering electronically with military computer networks" as an example of an act causing "military harm to another party," which could potentially make a civilian subject to attack for as long as he or she carries out such an act.[107] This example may, however, raise more questions than it answers. Which personnel working with computer programs and information systems are included in the description of "interfering electronically" with an adversary's computer networks? What are their duties? For how long are the individuals engaged in these and related computer or information processing activities susceptible to attack?

Conflict in cyberspace does not focus on the operation of conventional weapons but instead on the use of information through the deployment of malware and computer programs that include worms, viruses, logic bombs, and an infinite variety of other damaging data packages. Determining the participation of a civilian in hostilities based on the role he or she plays in managing and processing such information—as part of the deployment of a cyber weapon—may present much more complicated scenarios than those associated with conventional weapons that depend on the simple launching, motion, and impact of physical objects or the application of other physical forces.

While the parameters of IHL rules in this area remain uncertain, any broad definition of direct participation in hostilities, in the vast realm of cyber space, risks making many civilian personnel who work with interrelated and diverse types of information and information technologies susceptible to attack. This problem may be significantly complicated by the blurred line between personal and work-related activities that many civilian workers often cross as they process information on their laptop computers, iPhones, and other electronic means of accessing the Internet. Although individuals with laptops sitting in coffee shops may routinely pursue harmful cyber activities and may also undertake work-related activities involving state-sponsored cyber activities, the prospect of expanding an existing armed conflict by imposing the IHL regime on such individuals, potentially subjecting them to lawful attack, is an alarming prospect.

In terms of military operations, a large number of diverse technicians and specialists, many of them civilian, may routinely be involved in interrelated computer and information activities, potentially including those required to access enemy computer systems and direct harmful cyber actions against them. It is thus not

---

107. *Direct Participation in Hostilities: Questions and Answers*, INT'L COMM. OF THE RED CROSS (Feb. 6, 2009), *available at* http://www.icrc.org/eng/resources/documents/faq/direct-participation-ihl-faq-020609.htm.

surprising that the ICRC notes with concern the reality that a wide variety of civilian specialists may be called upon to assist members of the armed forces of a state in conducting a hostile cyber action.[108] A serious and daunting task will thus confront military planners and their legal staffs: determining which information-related activities by an enemy are so integral to military operations or "intrinsic to a particular cyber process" that they will make the personnel involved in those activities subject to attack based on their direct participation in hostilities.[109]

More broadly, such concerns highlight the dangers of imprudently extending the IHL framework to encompass many information activities. An overbroad application of the concept of direct participation in hostilities into the realm of information processing could in fact threaten the fundamental purposes of the IHL regime in the modern information age, potentially exposing vast areas of existing civilian activity to targeting and attack.

II. INFORMATION AS A WEAPON AND TARGET: PROBLEMS OF ACCESS AND CONTROL

A. *Accessing Information: "Acts of Violence" Against "Objects of Attack"?*

Rather than blasting or physically forcing its way into an adversary's systems or networks, a hostile cyber act uses information to persuade targeted systems or networks to grant admittance.[110] While these acts involve "penetrating" enemy systems or networks, they are commenced and conducted essentially as unauthorized acts of accessing information.

The nature of hostile cyber acts—in which information in systems and networks must first be accessed by "persuasion"—makes these acts highly unusual candidates for regulation under either the *jus ad bellum* or *jus in bello*. No physical objects are destroyed by the hostile cyber access itself; no planes, missiles, shells, bombs, or other physical objects fall on enemy forces or land on the territory of a

---

108. *See* DÖRMANN, *supra* note 23, at 8 (noting that "[t]here is a strong likelihood that civilians will be involved in [CNAs] often due to their specific technical expertise, which members of the armed forces may not necessarily have. This involvement can take a variety of forms.").

109. Charles J. Dunlap Jr., *Perspectives for Cyber Strategists on Law for Cyberwar*, 5 STRATEGIC STUD. Q. 81, 90 (2011).

110. MARTIN C. LIBICKI, CONQUEST IN CYBERSPACE: NATIONAL SECURITY AND INFORMATION WARFARE 35 (2007) (arguing that since computer networks are under the ultimate control of the owner, "there is no such thing as forced entry in cyberspace") (emphasis omitted).

foreign state; and no physical forces or physical objects are directed against the military forces of an adversary.

Countless acts of unauthorized access to computer systems and networks occur every day around the world (including diverse forms of cyber espionage), but these acts are routinely addressed as criminal, civil, or administrative matters under domestic laws and regulations—and not as acts of war that implicate the *jus ad bellum* and IHL framework.[111] However, as noted above, only illegal "acts of force" implicate the *jus ad bellum*, and only "the most grave" forms of the use of force satisfy the requirements for an armed attack justifying an armed response under the UN Charter. The most common characteristics and effects of illegally accessing computer systems and networks fall far short of the high standards for an armed attack under the *jus ad bellum*, even if one assumes that other key requirements, such as attribution, can be met.

Acts involving unauthorized access to computer systems and networks are also particularly difficult to reconcile with the model upon which the modern international legal system is founded: state sovereignty over territory. A nonphysical information "incursion" into an adversary's computer systems or networks is not equivalent to the invasion of another state's territory. Without such a physical incursion into anther state's territory by objects or enemy personnel, the negative effects of cyber actions lack a fundamental component of illegal uses of force as they are ordinarily assessed under the *jus ad bellum*.

In terms of the *jus in bello*, the legal threshold for the application of the IHL framework under the Geneva Conventions of 1949 is, as noted above, the presence of an "armed conflict." In the broadest terms, such a conflict can be said to exist "whenever there is a resort to armed force between States."[112]

Since armed force necessarily implicates some variation of a clash or contest of arms, the definition of *arms* plays a part in delineating the concept of "armed force." As noted above, the expansive phrase "weapon, means or method of warfare" appears to be able to encompass harmful cyber techniques, technologies, and computer programs. If so, the use of cyber weapons or techniques could qualify as a "resort to arms" between opposing military forces in an international armed conflict.

---

111. JAMES ANDREW LEWIS, CTR. FOR STRATEGIC AND INT'L STUDIES, THE CYBER WAR HAS NOT BEGUN 2 (2010), *available at* http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf ("Espionage and crime in cyberspace are routine occurrences, but they are not acts of war and do not justify the use of military force in response.").

112. Prosecutor v. Tadic, Case No. IT-94-1-AR72, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

Notwithstanding potentially broad definitions of *arms* and *armed conflicts*, the IHL framework was never intended to apply to every type of harmful, unfriendly, or unwanted action that states are capable of taking against each other. Instead, as emphasized by the ICRC, "IHL is the body of rules applicable when armed violence reaches the level of armed conflict, *and is confined only to armed conflict*."[113] The presence of "armed violence" is thus central to the IHL regime. Furthermore, the regime's obligations and restrictions are intended to apply to a specific type of armed violence: an attack.

The term *attack* has been correctly referred to as "of decisive importance" in the application of key IHL rules.[114] Protocol I, which represents the most widely accepted and authoritative statement of IHL obligations, does not define an attack merely in terms of harmful consequences; instead the protocol's Article 49 describes an attack as "[an] *act*[ ] of violence against the adversary, whether in offence or in defence."[115]

The emphasis on acts of violence in the text of Article 49 suggests that attacks are dependent on a finding of "physical force," thus excluding other harmful, nonphysical acts.[116] The ICRC interpretation in the *Commentary* to Protocol I simply confirms that "[t]he term 'attack' means 'combat action.'"[117]

Proponents of the proposition that harmful consequences alone determine the threshold for an attack have argued that the drafters of Protocol I did not envision modern military capabilities other than those involving "the immediate release of violent kinetic forces."[118] Yet it is unclear why "kinetic forces" alone—as opposed to the broader and more familiar concept of physical forces and objects—should be the key in making this determination.[119] Indeed, as reflected in the

---

113. *International Humanitarian Law*, *supra* note 10, at 722 (emphasis in original).

114. *Id.* The term *attack* is found sixty-seven times in the text of Protocol I.

115. Protocol I, *supra* note 22, at art. 49 (emphasis added).

116. MICHAEL BOTHE, KARL JOSEF PARTSCH & WALDEMAR A. SOLF, NEW RULES FOR VICTIMS OF ARMED CONFLICTS 289 (1982) (noting that "[t]he term 'acts of violence' denotes physical force. Thus, the concept of 'attacks' does not include dissemination of propaganda, embargoes, or other non-physical means of psychological or economic warfare."). Notwithstanding the authors' comments on the overall purposes of Protocol I, they properly note its unmistakable focus on "physical force." *Id.*

117. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 63, ¶ 1880.

118. Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, 4TH INT'L CONF. ON CYBER CONFLICT 283, 290 (C. Czosseck & Ziolkowski eds., 2012).

119. Weapon systems that utilize objects in motion, thus employing kinetic energy, are only one type of conventional weapon system now used by military forces in physical domains. As noted above, the U.S. Air Force uses the phrase "non-kinetic" to refer to actions "that produce effects without direct use of the force or energy of moving objects," thus excluding various conventional weapons such as those that utilize electromagnetic radiation or directed energy. *See* U.S. DEP'T OF THE AIR FORCE, AIR FORCE DOCTRINE DOCUMENT 2-5, INFORMATION OPERATIONS 116 (Aug. 5, 1998).

Commentary to Protocol I, the threshold for establishing an attack and an act of violence focuses on combat and physical force (which, in its most common understanding, involves the employment of physical forces or objects) and not on the narrower concept of kinetic forces.

From its formative stages, the IHL framework was not centered on the possible effects of many different types of harmful state conduct but instead on the physical violence associated with a broad range of weapons employing physical forces and objects (not merely "violent kinetic forces"). Thus, the foundational 1899 and 1907 Hague Conventions included not only restrictions on projectiles, munitions, and weapons employing kinetic forces but also a ban on the use of poison.[120] The employment of the destructive physical properties of both chemical and bacteriological (later biological) weapons was also formally banned soon after in the 1925 Geneva Protocol.[121]

In spite of the IHL regime's undisputed foundations on physical acts of violence, it has become fashionable among some writers to argue that hostile cyber acts should be included within the scope of attacks because cyber capabilities belong to a subset of physical weapons referred to as nonkinetic weapons.[122] In support of this proposition, operations involving chemical and biological weapons are incongruously cited as precedents for equating cyber weapons with "other" nonkinetic weapons on the basis of their destructive consequences.[123]

As noted, however, the historic focus in the IHL regime has been on physical forces and objects, which has always included a smaller subset of various nonkinetic, *physical* weapons, ranging from older versions, such as poison and dangerous pathogens, to modern versions, such as electromagnetic radiation and other directed energy weapons. Information weapons, which lack the legally significant

---

120. *See* Hague Convention (IV) Respecting the Laws and Customs of War on Land art. 22, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631; Hague Convention (IV) Respecting the Laws and Customs of War on Land, Annex (Regulations) art. 23(a), Oct. 18, 1907, 36 Stat. 2295, 1 Bevans 643; Hague Convention (II) Respecting to the Laws and Customs of War on Land, Annex (Regulations) art. 23(a), July 29, 1899, 32 Stat. 1811, 1 Bevans 252.

121. *See* Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T 571 (restating and reaffirming the prohibition on the use of chemical weapons and extending it to the use of bacteriological methods of warfare).

122. *See* WILLIAM H. BOOTHBY, WEAPONS AND THE LAW OF ARMED CONFLICT 238 (2009) (arguing that destructive CNAs qualify as "attacks" under Protocol I because that term is properly interpreted to "extend to violent consequences of an attack which does not consist of the use of kinetic force").

123. *See, e.g.*, Michael N. Schmitt, *Cyber Operations and the* Jus in Bello*: Key Issues*, 87 INT'L L. STUD. SERIES, U.S. NAVAL WAR. C. 89, 94 (2011) ("[I]t has always been the case that operations employing biological contagions or chemicals have been characterized as attacks, even though non-kinetic in nature, because their consequences could prove harmful, even lethal.").

physical attributes, characteristics, and capabilities of physical weapons, are another matter.

The fundamental differences between physical weapons and hostile uses of information are not usefully explained by referring to cyber capabilities as nonkinetic. This nonkinetic lens is equally unhelpful in explaining the critical differences between hostile cyber acts and the physical use of armed force for purposes of the *jus ad bellum*, although some authors employ this lens—again relying on the inapt comparison to biological and chemical weapons—to equate these acts on the basis of their destructive effects.[124]

State practice, to this point in history, continues to support the clear focus of the IHL framework on acts of physical violence (involving weapons that employ physical forces or objects) as opposed to a focus on merely the effects of many varied, harmful state actions. The process of accessing data in an unauthorized manner, however, bears little resemblance to the acts of physical violence that the IHL framework was designed to regulate.[125] The nonviolent nature of such cyber acts is reflected in the innumerable, diverse forms of unfriendly and damaging actions in cyberspace that occur, and will continue to occur, on a daily basis around the world outside of armed conflict and outside the IHL framework.

As noted, the international community has collectively decided to exclude a variety of harmful, nonphysical acts from both the *jus ad bellum* and IHL framework, including damaging acts of espionage, subversion, and political and economic coercion. In the absence of any state practice, it has nonetheless been argued that the IHL framework should be applied to nonphysical hostile cyber acts when they result in serious physical damages.

Yet to encompass within the IHL framework a vast new set of nonphysical actions—involving the uninvited accessing of information and then subsequent acts of denial of service, exploitation, or manipulation of data—is a highly significant and problematic step, one which remains dependent on state practice (in the continuing absence of any relevant international agreements). Significantly, not a single state has actually embraced this innovation with respect to

---

124. *See, e.g.*, Schmitt, *supra* note 44, at 573 (arguing that "[i]t would be no less absurd to suggest that cyber operations that generate consequences analogous to those caused by kinetic force lie beyond the [reach of the prohibition on the use of force], than to exclude other destructive non-kinetic actions, such as biological or radiological warfare"). Unlike information in computer codes, such WMDs have physical attributes and properties and utilize physical agents to cause harm. *See* THOMAS RID, CYBER WAR WILL NOT TAKE PLACE 13 (2012) (noting how some weapons, such as biological and chemical weapons, rely on neither physical force nor energy but instead on "agents" to do the work of harming targets).

125. Cyber techniques and methodologies may in fact broadly represent "a computer-aided assault on violence itself." *See id.* at xiv (further arguing that by offering various ways to achieve objectives without resorting to physical violence, "cyber attacks help to diminish rather than accentuate political violence").

real (as opposed to hypothetical) cyber incidents, in spite of the expanding universe of hostile cyber acts affecting the financial, industrial, and security interests of states, including acts targeting critical components of their national infrastructure.[126]

The nonviolent, nonphysical nature of a hostile cyber act itself is only one characteristic that makes such an act unusual for purposes of both the *jus ad bellum* and *jus in bello*. Another unusual characteristic concerns the diverse, highly ambiguous, and often temporary effects of these acts, which are directly related to the central role that information plays in constituting targets in cyberspace.

An immense array of potential information targets is emerging in cyberspace, accompanied by new cyber techniques capable of damaging, denying, or disrupting them. Governments apparently continue to direct their military forces and intelligence organizations to identify and pursue new opportunities to advance national security objectives by engaging in hostile cyber acts against many of these information targets.

New information targets of potential interest to the military include websites and other portals on the Internet used by adversaries—valuable targets that may be difficult if not impossible to destroy with physical force and conventional weapons. For example, the head of the U.S. Cyber Command and Director of the National Security Agency, General Keith Alexander, reportedly called for cyber capabilities to be used to block the publication of an "online jihadist magazine" because such a cyber action would be against "a legitimate counterterrorism target and would help protect U.S. troops overseas."[127] Along similar lines, even the U.S. State Department apparently has employed cyber capabilities to disable foreign websites associated with Al Qaeda.[128]

A state may thus perceive numerous military, security, or political advantages in undertaking hostile cyber acts that interrupt,

---

126. *See, e.g.*, STAFF OF CONGRESSMEN EDWARD J. MARKEY & HENRY A. WAXMAN, ELECTRIC GRID VULNERABILITY: INDUSTRY RESPONSES REVEAL SECURITY GAPS 11 (May 21, 2013) (noting that more than a dozen utilities in the United States reported "daily," "constant," or "frequent" attempted cyber attacks "ranging from phishing to malware infection to unfriendly probes;" that one utility reported that it was "the target of approximately 10,000 attempted cyber-attacks each month," and that other public power providers said that they "were under a 'constant state of attack' from malware and entities seeking to gain access to internal systems").

127. *See* Nakashima, *supra* note 21, at A3 (noting how British "cyber-warriors" reportedly temporarily succeeded in disrupting the website hosting the magazine and garbling its bomb-making instructions).

128. *See Hillary Clinton Boasts of US Cyberwar Against al-Qaeda*, TELEGRAPH (May 24, 2012), *available at* http://www.telegraph.co.uk/news/worldnews/al-qaeda/9286546/Hillary-Clinton-boasts-of-US-cyberwar-against-al-Qaeda.html ("In a rare public admission of the covert cyber war against extremists, the Secretary of State said cyber experts based at her department hacked Yemeni tribal websites, and took down messages about killing Americans.").

disable, or deny access to adversary websites and computer systems, even if the effects are temporary. Such temporary effects on these targets are, however, unlikely to meet the threshold for attacks under the IHL regime.

The view requiring a minimum threshold of damage in order for cyber acts to constitute attacks is widely held, and its proponents include some writers who advocate a consequentialist approach to cyber conflict.[129] However, it has also been suggested that a broad range of cyber actions that disable targets should also qualify as attacks.[130] A legal advisor at the ICRC has also suggested that specially protected objects, such as hospitals and medical units, must not only be protected from attacks but also from all harm and interference, arguably including low levels of cyber interference.[131] To argue, however, that various types of temporary cyber interference, annoyance, mischief, and disruption should constitute attacks subject to IHL restrictions risks dangerously overextending the IHL regime and further highlights the dangers of legally equating the informational with the physical.

While disruptive cyber acts may significantly interfere with activities that rely on timely access to denied information, the actual damages caused to targeted systems and networks are likely to be temporary in nature.[132] This phenomenon illustrates an important aspect of information as a target in cyberspace: unlike the natural environments of land, sea, air, and space, cyberspace is a human construct. This means that cyberspace is replicable, and thus damage to it can be repaired.[133]

The unusual, replicable character of cyberspace and the ambiguous effects of many hostile cyber actions are implicitly reflected in the once widely used term "computer network attack"

---

129. *See, e.g.*, Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 84 INT'L REV. OF THE RED CROSS 365, 374 (2002) ("[H]umanitarian law would not pertain to disrupting a university intranet, downloading financial records, shutting down Internet access temporarily or conducting cyber espionage, because, even if part of a regular campaign of similar acts, the foreseeable consequences would not include injury, death, damage or destruction.").

130. *See* DÖRMANN, *supra* note 23, at 6 (noting that since the definition of military objectives in Article 52.2 of Protocol I discusses "neutralization" of those objectives, "[i]t is irrelevant whether an object is disabled through destruction or in any other way").

131. *Id.* Protocol I provides that "[m]edical units shall be *respected and protected* at all times and shall not be the object of attack." Protocol I, *supra* note 22, at art. 11.1 (emphasis added).

132. *See* Martin C. Libicki, *Cyberwar as a Confidence Game*, 5 STRATEGIC STUD. Q. 132, 133 (2011) ("The direct effects of cyber attacks are almost always temporary. Rarely is anything broken (the Stuxnet worm perhaps a prominent exception). At the risk of a little oversimplification, because a cyber attack consists of feeding systems the wrong instructions, replacing such instructions in favor of the original correct instructions returns control to the owner.").

133. LIBICKI, *supra* note 110, at 5.

(CNA). CNAs have been 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."[134] Words like "disrupt" or "deny" may, of course, describe actions with only limited, temporary effects on the ability to access information.[135]

Hostile cyber acts encompassed by the term *CNA* may thus have consequences that range from serious damage to no damage at all. Within this range of effects, there are numerous types of nuisance, mischief, inconvenience, disruption, or denial that clearly do not rise to the level of armed attacks for purposes of attacks under the *jus in bello* or armed attacks under the *jus ad bellum*. Consequently, the term *CNA* is a poor tool for legal analysis, although it remains a useful illustration of the spectrum of events occurring in cyberspace.

The difficulty in equating temporary, disruptive cyber acts with armed attacks, even if undertaken on a massive scale against one country, is clearly reflected in current state practice. As noted above, the international community in general, and NATO states in particular, explicitly refrained from characterizing the disruptive cyber actions that paralyzed Estonia in 2007 as an armed attack or even as "a clear military action."[136] Such state practice stands, at least for now, in stark contrast to suggestions that if Russia were found legally responsible for the cyber actions against Estonia in 2007, the international community would or should have regarded them as illegal uses of force under the UN Charter.[137]

Evaluating the legal status of the effects of hostile cyber acts also focuses attention on the nature of the target. In implementing the fundamental principle of distinction, Protocol I requires that attacks be directed only against "military objectives," which are limited to "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[138]

---

134. DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, JOINT PUBLICATION 1-02, at 95 (amended through Apr. 2010).

135. Words like "degrade" and "destroy" imply more lasting damage, but as discussed in Part IV below, such terms require an examination of the targeted information (particularly its content and users) in order to determine if legal thresholds for armed attack or acts of violence are met.

136. *See* Traynor, *supra* note 35 ("Not a single [NATO] defence minister would define a cyber-attack as a clear military action at present.").

137. *See, e.g.*, CYBERATTACK WORKSHOP PROCEEDINGS, *supra* note 76, at 157 (arguing that "had Russia been responsible for [the cyber actions against Estonia] under international law, it is likely that the international community would (or *should* have) have treated them as a use of force in violation of the UN Charter and customary international law").

138. Protocol I, *supra* note 22, at art. 52, ¶ 2; *see also* CYBERATTACK WORKSHOP PROCEEDINGS, *supra* note 76, at 154.

In assessing the English text of Protocol I, the *Commentary* concluded that the word *object* refers to "something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing."[139] It further concluded that in both English and French, it was clear the word *object* "means something that is visible and tangible."[140]

The nonphysical objects of disruptive hostile cyber acts are thus highly unusual "objects of attack" for purposes of the IHL framework. The resulting effects may also be very difficult to categorize as the sort of physical damages (death, injury, or destruction of physical objects) that have long served as the basis for applying IHL obligations and restrictions. Even those who emphasize consequences in assessing the legal status of cyber acts may express reservations about treating data as an object of attack.[141] An additional, important, and unresolved issue hanging over the question of whether data can constitute an object of attack is the problem of its content, which is discussed in Part IV.

B. *Controlling, Confining, and Segregating Information*

Information, as it resides in or passes through cyberspace, may be much more difficult to control, confine, and segregate than physical objects and forces passing over or through the physical features of land, sea, air, and space. This characteristic ensures that information presents its own set of significant challenges related to the observance of the IHL principles of distinction and proportionality.

If in fact the IHL regime does apply to a particular cyber operation, those who plan or decide upon an attack must take various precautionary measures to ensure compliance with the principles of distinction and proportionality. These obligations require responsible planners and decision makers to, among other things, "do everything feasible" to verify that the objectives to be attacked are military objectives and not civilians or civilian objects; "take all feasible precautions in the choice of means and methods of attack" in order to avoid or minimize incidental damage or injury to the civilian population; and "refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life . . . which

---

139. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 63, ¶ 2007.

140. *Id.* ¶ 2008.

141. *See, e.g.*, Schmitt, *supra* note 123, at 96 ("Absent an agreed-upon interpretation in the cyber context, it is perhaps best to tread lightly in characterizing data as an object."). Similarly, for purposes of the *jus ad bellum*, see CYBERATTACK WORKSHOP PROCEEDINGS, *supra* note 76, at 154 ("[C]yber 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.'").

would be excessive in relation to the concrete and direct military advantage anticipated."[142]

Various methods that are available in conventional conflicts to evaluate whether a planned, ongoing, or completed attack complies with the proportionality principle are not available to the commander of a cyber operation. One fundamental problem is that cyberspace cannot be occupied in the same way that physical terrain can be controlled. This means that there is no guaranteed point, position, or space that can be occupied in such a way as to allow an attacker to observe and evaluate the effects of an attack—even after the attack has been launched.[143] Many types of information about a target may thus be less accessible to the commander of a cyber, as opposed to a conventional, military operation.

In both conventional and cyber military operations, a commander who is planning an attack and attempting to take "all feasible precautions" to minimize harm to the civilian population is not assumed to have access to perfect information. Instead, as explained by the ICTY, "In determining whether an attack was proportionate it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack."[144]

Although cyberspace is a domain of information, the "information available" to a reasonable commander who is planning an attack in cyberspace may ironically be extraordinarily limited. Commanders responsible for military cyber operations must deal with many challenges in observing the proportionality principle, including complex barriers that may prevent observation of the different levels of information that surround targets.[145] These barriers may impede efforts to evaluate the military value of targets while also obscuring connected and threatened civilian objects that are not the target of attacks, particularly when networks have both military and civilian functions.[146]

---

142. Protocol I, *supra* note 22, at art. 57.

143. In addition, it has been noted that "information about the effects of information warfare, besides being intrinsically hard to obtain, is itself subject to information warfare." LIBICKI, *supra* note 110, at 87.

144. Prosecutor v. Galic, Case No. IT-98-29-T, Judgment, ¶ 58 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 5, 2003).

145. *See* LIBICKI, *supra* note 110, at 94 (noting how "[c]hanging the architecture of the system can also throw off a determined [cyber] attacker. Networks can be rewired, routers might be added, internal addressing altered, and new internal barriers created to interfere with the attacker's ability to be certain the right target was attacked. . . . Firewalls and other filters may be present.").

146. *See* LIBICKI, *supra* note 78, at 153 (noting that "it may not always be obvious *when* a civilian target is being hurt. It is possible to know which military

Yet a commander remains under an obligation, to the extent feasible, to gather and evaluate information about potential targets to ensure compliance with IHL targeting rules. At a minimum, this involves a "continuing obligation to assign a high priority to the collection, collation, evaluation, and dissemination of timely target intelligence."[147]

Fundamental challenges, however, confront these efforts in cyberspace. Determining how to access an adversary's systems or networks to reach a specific target generally requires careful planning and substantial preparations. [148] Efforts to collect intelligence about those targets will also generally require penetrating enemy systems or networks to obtain information prior to the attack.[149]

However, an unauthorized entry into an adversary's computer systems for purposes of gathering intelligence may be viewed, if detected, as the attack itself. This dilemma highlights a problematic dimension of information when it is used to penetrate systems as a reconnaissance tool: the difficulty in characterizing the intent behind the intrusion.[150] Efforts to undertake precautionary measures that involve intrusions into enemy networks could thus, in the worst case scenario, prompt a counterattack by the enemy.

Even if an intrusion for purposes of gathering intelligence about a particular target is not viewed by an adversary as an attack, its detection could seriously threaten a commander's mission. Since such an intrusion may rely on the same methodologies and information to

---

functions a network supports without knowing what civilian services the same network supplies.").

147. BOTHE, PARTSCH & SOLF, *supra* note 116, at 363.

148. *See* LIBICKI, *supra* note 78, at 155 ("Cyberwarfare *qua* warfare is soaked in intelligence. . . . The search for vulnerabilities is usually a search for specific vulnerabilities in specific systems that can be exploited in specific ways. Intelligence is also needed on network architecture, the relationships between various defense systems . . . and influence relationships (what information affects which types of decisions?)"); Thomas Rid, *What Would a Real Cyberwar Look Like?*, NEW SCIENTIST (Sept. 15, 2013), *available at* http://www.slate.com/articles/health_and_science/new_scientist/2013/09/cyberwar_and_cyberattacks_it_s_really_espionage_subversion_or_sabotage.html ("[T]he number of violent computer-sabotage attacks against Western targets is zero. Why? Because causing havoc through weaponized code is harder than it looks. Target intelligence is needed.").

149. *See* CLAY WILSON, CONG. RESEARCH SERV., RL31787, INFORMATION OPERATIONS, ELECTRONIC WARFARE, AND CYBERWAR: CAPABILITIES AND RELATED POLICY ISSUES 5 (Sept. 14, 2006) ("Before a crisis develops, DOD seeks to prepare the IO [information operations] battlespace through intelligence, surveillance, and reconnaissance, and through extensive planning activities. This involves intelligence collection, that, in the case of IO, is usually performed through network tools that penetrate adversary systems to gain information about system vulnerabilities, or to make unauthorized copies of important files.").

150. *See* Jensen, *supra* note 86, at 235 (arguing that identifying the intent of the attacker is potentially more important because the state must "identify the attacker's intentions as hostile before it may respond with force in kind").

be used in a planned attack, its detection could risk compromising the means by which the attack is to be conducted—effectively shutting the "door" that had been opened into the enemy's networks or systems.[151]

A commander may thus face a serious dilemma if the requirement to take all feasible precautions is interpreted as requiring preliminary intrusions into an enemy's systems or networks. To the extent that feasibility relates to making an "informed decision" in this context, it will focus on what cyber intelligence-gathering operations must or can be conducted in order to make that informed decision.[152] However, a commander who undertakes an extensive intelligence-gathering operation as a precautionary measure may risk jeopardizing the planned mission by revealing methods or prompting countermeasures by an adversary who misinterprets the probe as the attack itself.

The contextual term "feasible" thus seems unlikely to require a commander to compromise his or her mission by penetrating an adversary's systems or networks as a precautionary measure. Given the lack of state practice, the contours of these rules in cyberspace are not yet clearly defined. Ostensible rules in cyberspace that defy compliance by reasonable commanders may be, however, just another kind of legal phantom.

More broadly, a commander seeking to comply with IHL obligations confronts formidable technical obstacles in precisely predicting the effects of hostile cyber actions. Because information is so inherently difficult to control, confine, and segregate in cyberspace, these obstacles exist even if the commander is equipped with the best intelligence available.[153] A variety of factors contribute to these obstacles and challenges. Unlike conflict in physical domains, conflict in cyberspace is not predictably constrained by physical laws such as those found in physics or chemistry; complex and rapidly changing operating systems can create conditions in which the same set of stimuli may not yield identical or even similar results, and cyberspace is a medium that can be quickly changed (by defenders or

---

151. *See* LIBICKI, *supra* note 110, at 35, 91 (noting how "[d]eep reconnaissance may trigger echoes that reveal holes to systems administrators, who can then plug them and thus change the vulnerability of the target;" moreover, since most computer network penetrations involve some sort of deception, such penetrations "can therefore be frustrated to the extent that deception can be unmasked").

152. *See* Eric Jensen, *Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?*, AM. U. INT'L L. REV 1145, 1184 (2003) (arguing that "feasibility" in cyber attacks "is really about what computer operations can legitimately be conducted to learn the intelligence needed to make an informed decision").

153. *See* LIBICKI, *supra* note 110, at 93 ("Yet, not even the best intelligence on opposing systems can provide perfect predictability of the consequences of an attack in cyberspace.").

by third parties).[154] Furthermore, various faults, holes, vulnerabilities, barriers, or anomalies in a particular system may be unknown to both attackers and defenders until that system actually confronts new, destructive, and unexpected information programs.

Another factor that may make even the best-planned hostile cyber act unpredictable is the human element. Humans are the key cyber players who may—or may not—detect hostile cyber actions, respond effectively to them, learn from them, make necessary adjustments to them, and be resistant or vulnerable to their methods of deception.[155]

Difficulties in predicting the consequences of a hostile cyber act may go far beyond understanding its immediate effects on targeted systems and networks. Information itself may be uniquely difficult to confine, particularly in view of the interconnected systems and networks that carry data in a "wired" modern society and global economy.[156] In this environment, where key networks and systems are becoming even more complex and interdependent, planners must grapple with the reality that the information they "launch" into cyberspace will confront no natural boundaries, may not easily be confined, and may be amenable to few, if any, certain controls.

The challenges in controlling information in order to limit damage to civilian objects in cyber operations are compounded by the other aspects of the nature of targets in cyberspace. It may be extremely difficult to segregate targeted information and information systems from those that are not to be targeted. While lines of communication used by the military are generally regarded as military objects, which are subject to attack, military communications rely heavily on the commercial communications infrastructure.[157]

The practice of some countries, including the United States, of broadly defining military objectives—by including objects that make "an effective contribution to the enemy's war fighting/war sustaining effort"—further broadens the list of dual-use targets for possible

---

154. *See id.* (likening the process to predicting the outcome of a chess game in which the board and pieces change).

155. *See id.* at 94 (describing the significant role played by the human element in information warfare).

156. *See* Evelyn Iritani & Thomas S. Mulligan, *U.S. Economic Slowdown Is Easing Its Way Around the Globe*, L.A. TIMES (Jan. 11, 2001), *available at* http://articles.latimes.com/2001/jan/11/news/mn-11033 (referring to the benefits corporations now enjoy in rapidly transmitting information and making immediate market-based adjustments in "a global, wired economy").

157. *See National Defense Authorization Act for Fiscal Year 2012: Hearing Before the Subcomm. on Emerging Threats and Capabilities of the H. Comm. on Armed Servs.*, 112th Cong. (Mar. 16, 2011) (statement of Gen. Keith B. Alexander, Commander, U.S. Cyber Command) ("The vast majority of our military's information packets ride on commercial infrastructure.").

hostile cyber actions.[158] In particular, based on their war-sustaining capabilities, various economic objects—including banks, stock exchanges, main export industries, and other key financial and corporate interests—may represent important targets for cyber capabilities within the framework of "effects based targeting."[159] Attacking such targets on this basis has, however, been intensely criticized.[160]

Nevertheless, cyber capabilities clearly provide new opportunities to conduct operations to destroy, or temporarily disable, these and many other objects that may have been previously inaccessible or impractical to attack with conventional weapons. Such cyber actions may not only be more effective than attacks with conventional weapons but will also have the ability to avoid causing various types of incidental physical damage (from fires, blast damage, chemical spillage, radiation, etc.) that pose a serious threat to civilians.[161]

In general, cyber capabilities represent important new tools for military forces to achieve results that were once only obtainable by conventional weapons.[162] In practical terms, they also add new types of objects of military value to target lists, including targets linked to economic resources upon which an adversary relies. These new targets, however, raise new questions about compliance with the principle of proportionality and the applicability of the IHL regime itself.

Regardless of their legal status, hostile cyber acts against targets of economic importance raise fears about new types of risks. These

---

158. COMMANDERS HANDBOOK ON THE LAW OF NAVAL OPERATIONS, *supra* note 115, ¶ 5.3.1; U.S. ARMY, JUDGE ADVOCATE GENERAL'S LEGAL CENTER AND SCHOOL, OPERATIONAL HANDBOOK ch. 2, § IX.A.2.b.(1) (2012) ("The connection of some objects to an enemy's war fighting or war-sustaining effort may be direct, indirect, or even discrete.").

159. *See* Tony Montgomery, *Legal Perspective from the EUCOM Targeting Cell*, 78 INT'L L. STUD. 189, 190 (2002) (explaining that "[e]ffects based targeting theorizes that by attacking specific links, nodes, or objects the effect or combination of effects will achieve the desired objective").

160. *See, e.g.*, MARCO SASSOLI, LEGITIMATE TARGETS OF ATTACKS UNDER INTERNATIONAL HUMANITARIAN LAW 6 (2003), *available at* http://www.hpcrresearch.org/sites/default/files/publications/Session1.pdf. *But see* Ruth G. Wedgwood, *Proportionality, Cyberwar, and the Law of War*, 76 INT'L L. STUD. SERIES, U.S. NAVAL WAR. C. 219, 222 (2002) (noting that "[e]conomic assets are considered military targets for their support of the war effort" and, despite criticism, "the legitimacy of weakening an adversary's industrial base and war production facilities is generally accepted").

161. *See* Jensen, *supra* note 18, at 1174 (further noting that CNAs "will be perceived as a less destructive use of force, in most cases, causing less collateral damage than kinetic weapons that accomplish the same task. Depending on the target, it will likely result in fewer injuries and deaths, limited physical destruction, and a quicker recovery after hostilities cease.").

162. *See* AIR FORCE, CYBERSPACE OPERATIONS, *supra* note 4, at ii ("Technological advances have provided the means to generate decisive and magnified effects in domains that traditionally could only be achieved via kinetic means.").

perceived risks include unwanted and disastrous effects on financial institutions worldwide, said to even inspire a sort of "unwritten international taboo" against cyber targeting of banking systems.[163] Such concerns may, in fact, have played a part in decisions by the U.S. government to forego possible cyber actions against some financial targets in several conflicts, including a contemplated action against the bank accounts of Serbian leader Slobodan Milošević during the Kosovo conflict in 1999 and against Iraq's financial system in 2003.[164]

While offering significant military advantages, hostile cyber actions against critical economic targets and other national infrastructure objectives may also pose serious risks due to the unpredictable effects of those actions against interdependent systems (particularly as the interdependence of systems upon which national infrastructures depend may not even be visible).[165] The possible extended consequences of a hostile cyber action (whether described as ripples, reverberations, or "second and third tier effects known as 'knock-on' effects")[166] on information in interconnected communications, energy, industrial, or financial systems could be far-reaching and hard if not impossible to reliably predict.[167]

Some commentators have suggested that technical solutions are available to improve the accuracy of cyber weapons and that it is possible to design highly discriminating and accurate cyber weapons.[168] However, as noted above, systemic challenges confront

---

163. *See* Ellen Nakashima, *Pentagon Officials had Weighed Cyberattack on Gaddafi's Air Defenses*, WASH. POST, Oct. 18, 2011, at A5 (discussing the context of the George W. Bush administration's consideration of taking cyber actions against Iraq in 2003 to dismantle the Iraqi financial system).

164. *See id.* (quoting a former Bush Administration official as saying that a planned cyber action to dismantle Iraq's financial system before the U.S. invasion was "blocked over concerns about collateral damage that might affect systems beyond the target").

165. *See* Richard G. Little, *Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures*, 9 J. URB. TECH. 109, 111 (2002) ("Mitigating damage to infrastructure and ensuring continuity of service is complicated by the interdependent nature of these systems. For example, although the interdependence of many systems is straightforward (e.g., the role played by electric power in providing other services is obvious), the interdependencies of other systems are no less real if not as visible.").

166. *See* Jensen, *supra* note 18, at 1149 (discussing suggestions for new international agreements that would accommodate the "unique aspects of CNA").

167. See Little, *supra* note 165, at 112 ("The potential for failures in one infrastructure system to cause disruptions in others that could ultimately cascade to still other systems with unanticipated consequences is very real. In truth, beyond a certain rudimentary level, the linkages between infrastructures, their interdependencies, and possible failure mechanisms are not well understood."); LIBICKI, *supra* note 110, at 259 (noting that "the more the world's economy becomes globalized, the harder it is to predict ripples from any one act of mischief").

168. *See, e.g.*, Forrest B. Hare, *Five Myths of Cyberspace and Cyberpower*, SIGNAL MAG., June 2007, at 90 (arguing that it is a myth that the effects of "cyberweapons are difficult to control").

efforts to ensure that harmful information will be effectively controlled or confined once it is used against complex, sensitive targets—particularly in view of unknown interconnected systems, anomalies and changes in those systems, unforeseen technical complications, and unpredictable human involvement.

Unpredictable human involvement includes the possibility that cyber actions will be misinterpreted and that responses to those actions will quickly and dangerously escalate. The "unique characteristics of cyberspace" (which include problems related to determining the intent behind cyber actions, anonymity, vast numbers of actors with malicious cyber tools, and the "the speed of action and dynamism inherent in cyberspace") may collectively make this danger of escalation across interconnected systems "especially acute."[169]

The DoD argues that "dangerous escalatory situations" can be prevented "by following the same policy principles and legal regimes in its cyberspace operations that govern actions in the physical world, including the law of armed conflict."[170] Because of the unique properties of information, however, this reliance on the law of armed conflict to successfully govern and control hostile cyber actions (based on perceived similarities with laws governing conventional weapons in physical domains) may be seriously overstated or misplaced.

The IHL obligations governing those who plan or decide upon attacks do not appear to include responsibility for all the possible, or even foreseeable, consequences of cyber attacks. Instead, based on the language found in Protocol I, the obligations appear to include only those effects that can be described as expected.[171] In particular, the language setting forth the scope of precautionary measures to ensure observance of distinction and proportionality requires those who plan or decide upon an attack to "refrain from deciding to launch any attack which may be *expected* to cause incidental loss of civilian life."[172]

This legal standard confining the scope of precautionary measures means that the effects of many military operations in

---

169. DOD CYBERSPACE POLICY REPORT, *supra* note 5, at 5.

170. *Id.* at 5, 8 (further noting that in spite of the challenges posed by the interconnected nature of cyberspace, "[t]he law of armed conflict and customary international law . . . provide a strong basis to apply [legal frameworks developed for specific physical domains] to cyberspace governing responsible state behavior").

171. Eric Jensen noted that

> [t]he international law standard for CNO is that a commander may use CNA if he, in good faith, believes that the damage to civilian objects and injury to civilians expected from the attack, given the circumstances as known to him at the time after taking all feasible measures to ascertain those circumstances, is not excessive to the concrete and direct military advantage anticipated.

See Jensen, *supra* note 18, at 1187.

172. Protocol I, *supra* note 22, at art. 57.2(a)(iii) (emphasis added).

cyberspace may simply remain outside the realm of the IHL framework—as legal phantoms in an unchartered area of serious and complex policy concerns. Nonetheless, concerns about collateral damage appear to be an important factor in continuing to restrain many cyber operations.[173] Even if the IHL regime is inapplicable, decision makers reasonably may be hesitant to approve hostile cyber acts with potentially far-reaching and unpredictable effects on information linked to diverse industrial facilities, communication centers, transportation hubs, commercial activities, financial institutions, and other unidentified organizations and activities around the world.

Beyond concerns that are arguably shaded to some degree by legal questions, various other fears appear to have limited the use of many cyber weapons by states.[174] One set of such extralegal fears has been the political and strategic consequences of being the first major power to launch a cyber attack, including the possibility that such an action will legitimize this new means of warfare.[175]

Other extralegal concerns that have apparently limited the use of cyber weapons relate directly to the peculiar status of information as a weapon, further illuminating yet another important aspect of its "uncontrollability." Unlike the payload of physical weapons that is destroyed or damaged in attacks, the information making up a cyber weapon generally remains intact after its use, allowing any adversary with the necessary knowledge and ability to reprogram that malware for its own use (making it, as noted, an "open source" weapon).

This phenomenon, along with the knowledge that use will ensure obsolescence, appears to be important in continuing to limit the use of some new cyber capabilities. Thus, in situations where national interest is not clearly at risk, a sophisticated cyber weapon has reportedly been likened by U.S. government officials to an expensive

---

173. *See* Nakashima, *supra* note 163, at A5 (reporting that a proposal to use cyber weapons to interrupt power sources to disrupt Libya's air defenses would have forced Pentagon officials to confront "accidently infecting other systems reliant on electricity, such as those in hospitals").

174. Unofficial accounts of U.S. involvement in the development of the Stuxnet virus hint at the risks states may take if they assume responsibility for hostile cyber acts. *See* Mikko Hypponen, *A Pandora's Box We Will Regret Opening*, N.Y. TIMES (June 5, 2012, 5:34 PM), http://www.nytimes.com/roomfordebate/2012/06/04/do-cyberattacks-on-iran-make-us-vulnerable-12/a-pandoras-box-we-will-regret-opening ("The downside for owning up to cyberattacks is that other governments can now feel free to do the same . . . . By launching Stuxnet, American officials opened Pandora's box. They will most likely end up regretting this decision.").

175. *See, e.g.*, Eric Schmitt & Thom Shanker, *U.S. Weighed Use of Cyberattacks to Weaken Libya*, N.Y. TIMES (Oct. 18, 2011), *available at* http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html (describing how U.S. officials reportedly "balked" at approving the use of cyber weapons to disrupt Libyan air defenses, fearing among other things that "it might set a precedent for other nations, in particular Russia or China, to carry out such offensives of their own").

car that is best left in the garage.[176] A final concern is also presented by the possibility that the use of a sophisticated cyber weapon will provide a clear indication of what might otherwise have been the secret capabilities of the attacker.[177]

Government, military, and intelligence officials must thus grapple with numerous risks as they weigh the strategic, security, and policy implications of using cyber weapons. These concerns, complicated and magnified by the unpredictability of cyber weapons and the inherent difficulty in controlling information, serve to constrain cyber operations. Although legal uncertainties about incidental damages may cloud assessments of many cyber actions, important policy issues also surround almost every aspect of their possible employment. In many cases, the IHL regime will simply not apply to hostile cyber actions, and even if it does, it is unlikely to apply to all of their effects. It has thus been suggested that while cyber activities present various legal challenges, "many problems masquerading as 'legal' issues are really undecided policy issues with a number of legal alternatives."[178]

III. INFORMATION AS A TARGET: THE PROBLEM OF EXPLOITATION AND CHALLENGES TO CONSEQUENCE-BASED LEGAL THRESHOLDS

A. *Exploitation: A Harmful—But Problematic—Act*

While legal concerns related to the observance of key IHL rules and principles, such as proportionality, distinction, and precautionary measures, in an attack are important, they are dependent on the larger threshold IHL problems presented by the use of information as a weapon and target. As noted, hostile uses of information can give rise to challenging, fundamental questions regarding the applicability of IHL itself. No actions highlight these questions more clearly than

176. *See id.* (quoting an unnamed U.S. official involved in the Libyan discussion as saying that "[t]hese cybercapabilities are still like the Ferrari that you keep in the garage and only take out for the big race and not just for a run around town, unless nothing else can get you there").

177. *See* Nakashima, *supra* note 163, at A5 ("In general, the U.S. government has been cautious in its deliberations over the use of cyberweapons, recognizing that using them can reveal capabilities and set precedents that might encourage other nations.").

178. Dunlap, *supra* note 109, at 90, 94 (further noting that in determining the incidental losses associated with cyber actions, "[a]ssessing second- and third-order 'reverberating' effects may be a wise policy consideration, but it does not appear LOAC currently requires such further analysis").

those encompassed within the concept of information "exploitation."[179]

The threshold question of whether the IHL regime applies to particular events in cyberspace is greatly complicated, if not dominated, by the nature of information itself and the problems presented by its content. Unlike other types of "targets" that may be attacked, information may have an intrinsic value that can be stolen or replicated through cyber methodologies and techniques. For this reason, the unauthorized exploitation of information by both state and nonstate actors is currently the most common and highly damaging type of unfriendly cyber action around the world.[180]

It has long been obvious that criminals can profit from exploiting valuable information that they access in computer systems and networks and that these illegal cyber activities have been extraordinarily costly for individuals and businesses.[181] Yet early fears expressed by U.S. officials about protecting cyberspace from cyber attacks tended to focus on the disastrous physical consequences of hypothetical, catastrophic cyber actions, while the damage from hostile cyber actions to this point has instead proven to be informational.[182]

Notwithstanding the obvious damage caused by physical forces, informational damages may be highly significant.[183] There is no

---

179. In its broadest sense, the term *information exploitation* may be defined as "[t]aking full advantage of any information that has come to hand for tactical, operational, or strategic purposes." *See* DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, *supra* note 134, at 170 (defining *exploitation*). In the more specific context of cyber operations, the commonly used term "Computer Network Exploitation" (CNE) refers to "intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary." *Id.* at 96.

180. *See* DOD CYBERSPACE STRATEGY, *supra* note 79, at 4 ("Every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies."); Libicki, *supra* note 27, at 54 ("It is fair to say the CNE accounts for the great preponderance of computer network operations carried out among states and similarly serious non-criminal organizations.").

181. *See* Editorial, *Cybersecurity at Risk*, N.Y. TIMES, July 31, 2012, at A22 (quoting General Keith Alexander, the chief of the United States Cyber Command and the director of the National Security Agency, as referring to the loss of industrial information and intellectual property through cyber espionage as "the greatest transfer of wealth in history").

182. *See* CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 12 (2008) (noting that advice from a U.S. Presidential Commission in 1998 on the protection of cyberspace "was not so much ignored as misinterpreted – we expected damage from cyber attacks to be physical (opened floodgates, crashing airplanes) when it was actually informational").

183. *See* Josh Rogin, *NSA Chief: Cybercrime Constitutes the "greatest transfer of wealth in history"*, FOREIGN POL'Y (July 9, 2012), *available at* http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history ("U.S. companies lose about $250 billion per year through intellectual property theft, with another $114 billion lost due to cyber crime, a number that rises to $338 billion when the costs of down time due to crime are

doubt that the exploitation of information—including military secrets and other classified information, intellectual property, financial records, and commercial data—in cyberspace is a growing and serious threat to both states and businesses.[184]

While state-sponsored efforts to access, steal, copy, or otherwise exploit critical information in an adversary state's computer systems and networks may constitute a new and important chapter in the long history of espionage, such acts are unlikely to violate any obligations under international law.[185] Furthermore, under the IHL framework itself, "information-gathering activities" have long been explicitly recognized as legitimate actions by military forces.[186]

Information can, however, be exploited in ways that cause great damage to states, even if such exploitation or cyber espionage does not amount to "war."[187] The acquisition and misuse of a state's most highly classified information regarding its deployed forces, military facilities, planned military operations, strategic policies, weapons capabilities, personnel records, intelligence activities, and key defensive vulnerabilities can all result in disastrous tactical and strategic consequences for that state, including events that may involve great loss of life and destruction of property.

Devastating consequences alone, however, cannot serve as the basis for imposition of the IHL framework on such acts. The nature of the act itself—the exploitation of information—is not the type of conduct that was intended to be subject to IHL restrictions, regardless of its highly damaging effects.

The exploitation of information thus serves to illustrate how analogies drawn between harmful cyber techniques and conventional weapon systems may be misplaced, particularly to the extent that they focus primarily on their harmful consequences. For purposes of the IHL regime, damaging acts of information exploitation—which

---

taken into account, said [General] Alexander, the director of the National Security Agency and commander of U.S. Cyber Command, in remarks Monday at the American Enterprise Institute.").

184. *See* DOD CYBERSPACE STRATEGY, *supra* note 79, at 3 ("Foreign cyberspace operations against U.S. public and private sector systems are increasing in number and sophistication. DoD networks are probed millions of times every day, and successful penetrations have led to the loss of thousands of files from U.S. networks and those of U.S. allies and industry partners.").

185. *See* Jeffrey H. Smith, *State Intelligence Gathering and International Law: Keynote Address*, 28 MICH. J. INT'L L. 543, 544 (2007) ("[I]t is fair to say that the practice of states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law.").

186. *See* Hague Convention (IV) Respecting the Laws and Customs of War on Land, Annex (Regulations), *supra* note 120, at art. 24 (providing that the "employment of measures necessary for obtaining information about the enemy and the country are considered permissible").

187. *See* Rid, *supra* note 3 ("Data breaches are not just a risk, but a real bleeding wound for the United States, Europe, and other advanced economies. But espionage is not war, and cyberespionage is not cyberwar.").

are often described as some form of cyber espionage—are legal phantoms: examples of varied, sometimes highly damaging, extralegal actions in cyberspace.

Cyber espionage and other forms of data exploitation are routinely addressed by states as criminal matters.[188] They further bear little resemblance to conventional methods and means of warfare, although they may have highly damaging consequences. This paradox appropriately focuses attention on the legal thresholds that must be met in order to apply the IHL framework to hostile cyber acts. As noted, writers who emphasize the importance of consequences generally view cyber acts of disruption and denial as inappropriate candidates for the IHL framework because of their limited or temporary effects. The highly damaging consequences of acts of cyber exploitation, however, necessarily focus attention on the legal significance of the underlying *acts*.

B. *Information Exploitation, Legal Thresholds, and Consequentialist Approaches to the* Jus ad Bellum

The unusual characteristics of cyber weapons have, as noted, given rise to considerable discussion among scholars regarding the question of whether cyber actions alone could ever qualify as an armed attack for purposes of the *jus ad bellum* and the use of armed force in self-defense under the UN Charter. In spite of the clear focus in the text of the UN Charter on a specific act (an armed attack) as the legal basis for a state's right to use force in self-defense, some scholars and experts have instead emphasized the destructive consequences of the act.[189]

This consequentialist or effects-based analysis has been described as "the leading view" among legal experts in determining whether a hostile cyber act constitutes an armed attack for purposes of the *jus ad bellum*, and, by extension, whether threshold requirements are also met for the application of the IHL regime.[190]

---

188. *See, e.g.*, 18 U.S.C. § 793 (2013) (criminalizing actions such as the obtaining, possessing, transmitting, or receiving of "information relating to the national defense" with "intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation").

189. *See, e.g.*, Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 103 (2002) ("The crux of the matter is not the medium at hand (a computer server in lieu of, say, an artillery battery), but the violent consequences of the action taken."); Schmitt, *supra* note 44, at 588–89 ("A cyber attack standing alone will comprise an armed attack when the consequence threshold is reached. . . . So long as a cyber operation is likely to result in the requisite consequences, it is an armed attack.").

190. *See, e.g.*, Dunlap, *supra* note 109, at 85 ("The leading view, therefore, among legal experts focuses on the consequences and calls for an *effects-based* analysis of a particular cyber incident to determine whether or not it equates to an 'armed

Other analytical approaches that equate various hostile cyber acts with conventional armed attacks, such as the "strict liability approach" and even some interpretations of the "instrument-based approach," also draw heavily, if not exclusively, on assessments of the consequences of cyber acts.[191]

Although the U.S. government has not definitively set forth criteria for determining the legal status of hostile cyber actions under the *jus ad bellum*, a consequentialist approach nonetheless prevails in much of its analysis.[192] Such an approach is also reflected in reported discussions of responses to cyber acts under the doctrine of "equivalence."[193]

However, a legal approach that focuses only on the consequences of cyber acts fails to account for the many ways in which information can be used to cause great damage to an enemy, even though the underlying acts clearly remain outside the recognized legal boundaries of armed conflict and the *jus ad bellum*. In this regard, cyber espionage and other increasingly varied, sophisticated, and damaging forms of cyber exploitation deserve special attention.

As noted above, exploiting the most highly classified military secrets of an adversary can cause destruction, defeats, and losses of monumental significance. One need only look at the intelligence activities of the Allies in World War II to appreciate the importance—and destructiveness—of intercepting, stealing, and otherwise exploiting critical information, particularly signals and secret codes.[194] The older, conventional underlying methods of espionage

---

attack' as understood by Article 51."). *See generally* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013).

191. *See* Graham, *supra* note 83, at 91–92 (reviewing the effects-based and strict liability models as well as the effects-oriented interpretations of the "instrument-based" model). *But see* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1041 (2007) (noting how "the classic 'instrumentality' approach argues that [an information operation] does not qualify as armed force because it lacks the physical characteristics traditionally associated with military coercion").

192. *See, e.g.*, OFFICE OF GENERAL COUNSEL, DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (May 1999), *reprinted in* THOMAS WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 431, 453 (2000) ("[I]t seems likely that the international community will be more interested in the consequences of a computer network attack than its mechanism.").

193. *See* Gorman, *supra* note 7 ("One idea gaining momentum at the Pentagon is the notion of 'equivalence.' If a cyber attack produces the death, damage, destruction or high-level disruption that a traditional military attack would cause, then it would be a candidate for a 'use of force' consideration, which could merit retaliation.").

194. *See, e.g.*, F. W. WINTERBOTHAM, THE ULTRA SECRET 2 (1974) (quoting the supreme allied commander in World War II, General Dwight D. Eisenhower, as describing "ULTRA" (wartime signals intelligence obtained by the breaking of high-level encrypted enemy radio and teleprinter communications) as having been "decisive" to the Allied victory); LIBICKI, *supra* note 110, at 28 n.21 ("A venerable uncle of

and intelligence gathering—which included electronic surveillance, code-breaking efforts, and various types of covert actions—have been supplemented and dramatically improved by modern cyber espionage techniques, sometimes with devastating consequences.[195]

Damaging acts of espionage and other unfriendly forms of information exploitation abound in modern international relations, along with other destructive, nonphysical acts designed to exert economic or political coercion. Because of the frequency, nature, and diversity of these unfriendly acts, imposing the *jus ad bellum* on all of them would diminish restrictions on the use of force, thereby significantly weakening key safeguards upon which the international community relies and undermining the UN Charter's central purpose of maintaining international peace and security.[196]

Such concerns influenced the drafters of the UN Charter as they grappled with *jus ad bellum* issues. Although they understood that many acts in the international arena can cause great harm to states, they decided that the UN Charter's central prohibition in Article 2(4) should be against the "threat or use of force."[197]

While the focus in Article 2(4) is on physical armed force, the phrase "use of force" is not defined in the UN Charter itself. It is nonetheless possible to identify some important, widely accepted parameters of the phrase. For example, efforts by a few states to explicitly include one important type of destructive, nonphysical conduct in the Article 2(4) prohibition against force—acts of economic coercion—were rejected.[198]

Thus, the consequences of unfriendly acts by states have not dominated the development of legal frameworks regarding recourse to force adopted by the international community. Instead, the consensus

---

computer network exploitation, codemaking and codebreaking, can also be associated with information warfare.").

195. *See Cyberwar: War in the Fifth Domain*, *supra* note 36, at 26 (quoting James Lewis of the Centre for Strategic and International Studies as referring to cyber espionage as "the biggest intelligence disaster since the loss of the nuclear secrets [in the late 1940s]").

196. *See* Hollis, *supra* note 191, at 1040 (arguing that the exclusion of economic and political forms of coercion from the definition of force "reflects an effort to proscribe those acts most likely to interfere with the U.N.'s primary purpose—maintaining international peace and security").

197. *See* U.N. Charter art. 2, ¶ 4 ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").

198. The Brazilian delegation proposed that Article 2(4) include a prohibition against the use of "economic measures," but this proposal was rejected by states during the drafting of the UN Charter. *See* Eleventh Meeting of Comm. I, Doc. 784, I/1/ XXVII U.N.C.I.O. Docs. 335 (June 4, 1945) (rejecting the Brazilian delegation's suggested inclusion of a prohibition against "economic measures"); Amendments to the Dumbarton Oaks Proposal Presented by the Brazilian Delegation, Doc. 2, 617(e)(4), III U.N.C.I.O. Docs. 251, 253–54 (May 6, 1945).

that emerged in framing the UN Charter, despite the objections of a small number of states, was that Article 2(4) should not be extended to include some important and damaging actions states may employ against each other, including acts involving destructive economic coercion.[199]

Although it is generally accepted that acts of economic coercion—like other hostile acts not involving physical armed force—lie outside the scope of Article 2(4), the effects of the most serious economically coercive measures may still be significant and highly damaging to the targeted states. Nonetheless, such damaging acts, and many other "non-military techniques of coercion," are generally classified by the international community not as illegal uses of force but instead as violations of the principle of nonintervention.[200]

Some proponents of a consequentialist approach to conflict in cyberspace suggest that the emphasis in Article 2(4) on a particular prohibited type of instrument—that is, force—is outdated or misplaced and should instead be viewed as a sort of "cognitive short hand" for the real issue that states are focused on: "destructive consequences."[201] It is also possible, however, to view the word "force" as conveying what appears to be its plain meaning in the text: physical armed force.[202] In this sense, it is a cognitive transcription of the desire of states to limit the most serious prohibitions and penalties of the UN Charter to the instrument whose misuse gave rise to the UN Charter regime in the first place.

The failure by states to include acts of espionage and acts of political, psychological, or economic coercion within the scope of Article 2(4) helps illustrate this point. Although these acts are not regarded as uses of force under the UN Charter, they may cause enormous damage. In particular, human rights groups and relief organizations continue to stress the highly damaging effects of coercive economic actions against civilians in targeted states. For example, some medical experts have argued that the U.S. embargo

---

199. *See* Richard B. Lillich, *The Status of Economic Coercion Under International Law: United Nations Norms*, 12 TEX. INT'L L.J. 17, 19 (1977) ("[There is little evidence to show that more than a handful of states in the UN ever have considered, much less now believe, that article 2(4) speaks to economic coercion.").

200. *See* Derek W. Bowett, *Economic Coercion and Reprisals by States*, 13 VA. J. INT'L L. 1, 1 (1972) ("[I]t is better to confine Article 2(4) to military force, including possibly the encouragement or incitement of military force, and to leave the issues of economic aggression or other non-military techniques of coercion to the separate principle of non-intervention.").

201. *See* Schmitt, *supra* note 44, at 573 ("The interpretive dilemma is that the drafters of the Charter took a cognitive shortcut by framing the treaty's prohibition in terms of the *instrument* of coercion employed—force. . . . Yet, it is seldom the instrument employed, but instead the *consequences* suffered, that matter to states.").

202. *See* D. W. BOWETT, SELF-DEFENSE IN INTERNATIONAL LAW 148 (1958) ("Taking the words in their plain, common-sense meaning, it is clear that, since the prohibition is of the 'use or threat of force', they will not apply to economic or political pressure but only to physical, armed force.").

against Cuba has "dramatically harmed the overall health and nutrition of many Cuban citizens."[203] Similarly, according to some reports, UN economic sanctions on Iraq from 1990 to 2003 had "devastating effects on the Iraqi population and economy."[204]

State practice related to economic and other nonmilitary, coercive measures helps demonstrate several important points. It establishes that a coercive or unfriendly action by a state that hurts another country's military forces or civilian population does not, on that basis alone, make the action a use of force or an act of aggression. This state practice further illustrates how international law has long distinguished between traditional uses of armed force and other types of acts involving the infliction of hardship or suffering.[205]

In spite of the great damage that may be caused by acts of economic coercion and by other nonphysical, unfriendly acts, writers applying a consequentialist approach generally do not regard such acts—or cyber operations involving them—as constituting a use of force.[206] This position is not based, however, on the absence of physical armed force but rather on various factors related to the effects of the acts. These factors include: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[207] While these factors may offer some useful insights, they fail to fully account for the unique properties of the information used in hostile cyber acts and also disregard the importance that states continue to attach to the nature of the *act* causing the harmful consequences.

The first factor, severity—relating to the scale, scope, and duration of the consequences—restates a legal requirement that is routinely applied in evaluating conventional uses of force. For example, as noted above, the ICJ distinguishes "the most grave forms

---

203. *See, e.g.*, Javier H. Campos, *The Impact of the U.S. Embargo on Health Care in Cuba: A Clinician's Perspective*, 14 TRANSNAT'L L. & CONTEMP. PROBS. 517, 519 (2004) (citing a study by the American Association for World Health examining the embargo's negative effects in various health-related areas, including "malnutrition, water quality, medicines, equipment, and medical information").

204. *See* LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN & KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW 19 (1998) (discussing the effects of the UN embargo against Iraq).

205. *See id.* at 18 (noting that "[l]ongstanding international practice recognizes that nations may inflict great hardship upon each other and their respective citizenries without such infliction constituting the use of force or a violation of international law").

206. *See, e.g.*, Schmitt, *supra* note 44, at 574 ("Whatever force is, then, it is not economic or political pressure. Therefore, a cyber operation that involves such coercion is definitely not a prohibited use of force.").

207. *See id.* at 575–77 (discussing factors "likely to influence assessments by states as to whether particular cyber operations amounted to use of force"); Dunlap, *supra* note 109, at 85 (noting that "Schmitt pioneered this [consequentialist] approach and offers seven factors to consider in making the judgment as to whether a particular cyber event constitutes 'force' at all").

of the use of force" from "other less grave forms" in order to determine the presence of any armed attack for purposes of Article 51.[208] The most severe damages caused by the most serious acts of economic coercion (and presumably also by other nonmilitary techniques of coercion) may be grave, but they are not the result of a prohibited use of force because—according to consequentialist analysis—they fail to comport with various other factors, such as directness, immediacy, and measurability.

A consequentialist approach posits that damages caused by economic actions are unlike those caused by conventional weapons, such as the damage from an explosion, because of an attenuated and indirect "causal connection."[209] It may indeed be difficult to determine the chain of causation for the eventual downturn of an economy based on the workings of complex market forces and government decision making in sanctioned countries. Yet the causal connection between some acts of economic coercion and their effects—such as an embargo causing the abrupt end of a state's ability to export a dominant commodity—may not be difficult to establish. At the same time, the perceived "directness" of many destructive cyber acts may be an illusion, as discussed in more detail in Part IV.

The temporal aspect of indirect—and thus delayed—consequences of economic and other nonphysical coercive or hostile actions gives rise to the so-called immediacy factor. Consequentialists suggest here that "states harbor a greater concern about immediate consequences than those that are delayed or build slowly over time."[210] Yet it is not at all clear that states regard delayed damages caused by physical weapons as any less serious from a legal or policy perspective than those with immediate consequences. For example, states have expressed great concern about the terrible damage that landmines may cause over many years and about the slow but deadly spread of pathogens linked to the employment of biological weapons.[211]

With respect to measurability, it is suggested that it is more difficult to identify or quantify harm caused by economic coercion

---

208. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶¶ 191, 195 (June 27); *see also* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 51 (Nov. 6) (strongly reaffirming the distinction made by the I.C.J. in *Military and Paramilitary Activities in and Against Nicaragua*).

209. *See* Schmitt, *supra* note 44, at 576 (contrasting causal attributes of economic and armed actions).

210. *Id.*

211. Such damages are in fact so serious that the international community has acted to ban both these weapon systems in international conventions. *See* Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163 [hereinafter Biological Weapons Treaty]; Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction, Sept. 18, 1997, 36 I.L.M. 1507 [hereinafter Ottawa Treaty].

than it is to do so for damage caused by physical weapons.[212] While this may be true in calculating more complex damages, such as those presented by economic opportunity costs, the sudden loss of funds in a country's foreign exchange bank can be immediate, highly damaging, and directly linked to actions preventing the export of goods. On the other hand, measuring the precise damages caused by some highly destructive physical weapon systems, such as those caused by biological agents, may not be as easy or simple.[213]

The great difficulty in successfully applying various factors to distinguish the consequences of hostile, nonphysical acts, such as coercive economic acts, from the effects of conventional, physical weapons (and attempting, in turn, to use these factors to distinguish the effects of cyber acts) highlights two critical issues. First, the act—and not just the consequences—matters. Second, when applied to the use of information as a weapon and target, some of these factors are merely signposts of intractable problems confronting attempts to analogize informational acts in cyberspace with conventional, physical weapons.

For example, responsibility as a factor takes on far more complex dimensions in cyberspace than it does in the physical world. As discussed above, responsibility and attribution problems are integrally linked to more difficult and fundamental problems presented by hostile uses of information and the architecture of the Internet itself. These problems cast long shadows over efforts to classify hostile uses of information as illegal uses of force.

When information is used as a weapon, invasiveness as a factor of analysis also highlights much larger, more complex problems presented by the use of information as a weapon than those presented by the use of physical weapons on physical terrain. Cyber weapons and acts of cyber espionage may in fact be highly invasive, yet involve no physical breach of territorial boundaries.[214]

A final consequentialist factor posits that since various unfriendly, harmful acts between states—including those involving propaganda, psychological warfare, or espionage—are clearly not

---

212. Schmitt, *supra* note 44, at 576–77.

213. Due to the difficulty of differentiating biological attacks from naturally occurring epidemics or endemic disease, such attacks have proven to be difficult to measure or even prove as evidenced by the inability of both the United States and the Soviet Union to gather convincing evidence to prove or disprove allegations of biological weapon attacks during the Cold War. *See* George W. Christopher et al., *Biological Warfare: A Historical Perspective*, 278 J. AM. MEDICAL ASS'N 412, 414–16 (1997) (noting that most of the allegations of biological attacks that have been made since World War I "have not been confirmed in the absence of compelling microbiological or epidemiologic data supporting a biological attack").

214. *See* Schmitt, *supra* note 44, at 576 (admitting that "[i]n the cyber context, [invasiveness] must be cautiously applied" since cyber exploitation is "highly invasive" and a "pervasive tool of modern espionage," yet clearly does not constitute a use of force).

regulated by international law governing the use of force, to the extent that such acts are conducted by means of cyber operations, they are "presumptively legitimate."[215] This argument, however, involves somewhat circular reasoning, while also skirting the central issue of what constitutes prohibited armed force. The harmful cyber acts at issue may be presumptively legitimate precisely because they, along with other cyber acts, do not involve the harmful, physical acts that are the focus of the *jus ad bellum*.

Complex combinations of factors that are said to inform a consequentialist approach to the *jus ad bellum* in cyberspace thus belie a simpler truth (and dilemma): legitimate cyber attacks must closely resemble not only the effects but also the *acts* that make up conventional armed attacks (involving physical armed force).

Notwithstanding their highly damaging consequences, hostile cyber acts involving unauthorized access to information—and subsequent acts of exploitation—again bear little resemblance to the acts involving physical armed force that have long served as the basis for the *jus ad bellum*. Instead, they rank among other nonphysical, coercive, or hostile acts that the international community has prudently chosen not to classify as state behavior justifying an armed response. To do otherwise risks undermining the UN Charter regime and the *jus ad bellum* itself.

C. *Information Exploitation, Legal Thresholds, and Consequentialist Approaches to the* Jus in Bello

Turning to the *jus in bello*, varied and complex forms of information exploitation pose serious challenges to an effects-based analysis in determining the legal status of hostile cyber actions. As discussed above, the initial threshold for the application of the IHL framework is the presence of an armed conflict. Consequentialist writers suggest that the key factors in finding that hostile cyber actions standing alone give rise to an armed conflict are essentially the same as those required for an armed attack for purposes of the *jus ad bellum*: destructive consequences (specifically, "measures that injure, kill, damage or destroy").[216]

Serious physical damages are indeed fundamental to an armed conflict. But the IHL regime was never intended to apply to every type of damaging action, including acts of information exploitation with highly destructive consequences. This is true because, as noted, the IHL regime speaks to both damaging consequences and

---

215. *Id.* at 577.

216. *See, e.g.*, Schmitt, *supra* note 76, at 174 ("Applying the approach adopted in the context of the *jus ad bellum*, relevant actions must be likely to result in injury, death, damage or destruction to comprise an international armed conflict.").

recognized acts, with a central focus on armed violence. In the context of an ongoing armed conflict, the key threshold question for application of the IHL framework focuses on a particular *act* of armed violence: an attack. For purposes of the IHL framework, Protocol I defines an attack as an "*act* of violence against the adversary, whether in offence or in defence."[217]

Any decision to apply the IHL framework to a particular hostile cyber action must thus be based on a careful assessment of the nature of the action to determine if it qualifies as an attack and an act of violence. In spite of the explicit focus of the IHL regime on the nature of the act, writers advancing a consequentialist approach instead focus on destructive effects. They thus view the term *attacks* as merely "prescriptive shorthand" for specific consequences and the term *violence* as "useful shorthand" for consequence-based rules designed to protect the civilian population from harmful effects.[218]

Such an approach problematically assumes that the phrase "act of violence" is merely explanatory (only in terms of its consequences) and not a legal requirement with separate components.[219] While it is clear that the core principles of the IHL framework seek to protect the civilian population from injury, death, damage, and destruction, the framework was not designed—and cannot be legitimately extended—to encompass all forms of serious, harmful state conduct in the cyber age. This is especially true regarding acts of espionage or information exploitation; such acts are widely recognized as lying outside the *jus ad bellum,* and as information-gathering activities they enjoy explicit protection under the *jus in bello.*

In light of the central role that physical violence plays in key IHL obligations and in related state practice, it is unclear why shorthand or shortcuts around this requirement are needed or desirable. On the contrary, such shorthand risks dangerously overextending the IHL framework to encompass cyber actions that it should not, particularly those involving complex and varied forms of information exploitation.

Writers applying effects-based analysis conclude that acts of cyber espionage should be excluded from the IHL framework because the "foreseeable consequences" of these acts generally "would not

---

217. Protocol I, *supra* note 22, at art. 49 (emphasis added).

218. *See, e.g.*, Schmitt, *supra* note 129, at 377 ("'Attacks' is a term of prescriptive shorthand intended to address specific consequences."); Schmitt, *supra* note 123, at 93 (noting that the primary purpose of the Additional Protocol was the protection of civilian populations and that "'[v]iolence' merely constituted useful prescriptive shorthand for use in rules designed to shield the population from harmful effects").

219. *See* Schmitt, *supra* note 129, at 377 ("To the extent that the term 'violence' is explicative, it must be considered in the sense of violent *consequences* rather than violent *acts*.").

include injury, death, damage or destruction."[220] Yet, diverse and complex types of information exploitation tools now challenge the simplistic classification of many hostile cyber actions and may even cause identical results.

Cyber techniques designed to exploit information may closely resemble many other types of hostile cyber acts and may in fact be difficult to distinguish in key respects.[221] Like other hostile cyber acts, information exploitation first requires an unauthorized intrusion into an adversary's systems or networks and may also require the clandestine placement there of malignant computer programs (for purposes of collecting and then transmitting information necessary for further hostile actions).

When hidden malware programs in an adversary's computer systems or networks exploit data by taking or removing it (and not by simply copying it), the damaging effects may be the same as those caused by other cyber acts stylized as destructive cyber attacks. When data is exploited because of its valuable content (particularly financial, intellectual, and proprietary information, as discussed in Part IV), even more difficult questions are raised in distinguishing cyber acts of exploitation and destruction.

If, in fact, the "taking" of information through its exploitation causes damage by reason of the loss of the value of that information, it becomes almost impossible to distinguish the destruction of that information in a cyber attack from an act of cyber espionage. There also remains the intractable problem of defining precisely what constitutes the "valuable content" of information for purposes of defining an attack and whether such data can or should serve as an object of an attack.

Content definition issues are, however, only one serious challenge to consequentialist attempts to distinguish acts of cyber exploitation from so-called cyber attacks. The status of this former set of cyber acts is also greatly complicated by the central and growing role that information exploitation (or exfiltration) plays in a wide variety of destructive hostile cyber actions. The destructive elements of the most sophisticated "offensive cyberweapons" may in fact be

---

220. *See id.* at 374 ("[H]umanitarian law would not pertain to disrupting a university intranet, downloading financial records, shutting down Internet access temporarily or conducting cyber espionage, because, even if part of a regular campaign of similar acts, the foreseeable consequences would not include injury, death, damage or destruction.").

221. *See* LIBICKI, *supra* note 110, at 28–29 (noting that "computer network attack and exploitation are close cousins. Both use similar tricks to get into information systems, and therefore call on similar skills. Both subvert control systems. But their intent in different.").

intertwined with necessary layers of "reconnaissance and espionage software," which collectively make up the "attacking software."[222]

Cyber exploitation software may thus be indistinguishable from the destructive malware itself and the operational parameters may be similar as well—the only difference being the "payload" that is to be executed.[223] It is also possible that individual malware payloads may simultaneously have "multiple functions," one designed to exfiltrate data and the other to destroy or manipulate it, depending on which commands are received or how the malware is otherwise controlled.[224]

Many complex cyber weapons may depend on the successful exfiltration of data in order to cause intended damage. As reportedly demonstrated by the Stuxnet worm, manipulating data in complex computer systems at highly secure, secret facilities is likely to require extensive reconnaissance activities and planning—making the data exploitation process essentially the first part of the strike itself.[225]

Cyber tools designed for exploitation purposes continue to become more complex, sophisticated, and damaging. These developments are demonstrated by the "Flame Virus," which has been described by government officials as a "massive piece of malware" that "secretly mapped and monitored Iran's computer networks, sending back a steady stream of intelligence to prepare for a cyberwarfare campaign."[226] The Flame Virus is said to further illustrate the importance of "mapping networks and collecting intelligence on targets as the prelude to an attack, especially in closed computer networks."[227] While the Flame Virus may be both a powerful and unprecedented tool of cyber espionage as well as the first part of a larger hostile cyber act, it may also be able to perform

---

222. Randall R. Dipert, *The Ethics of Cyberwarfare*, 9 J. MIL. ETHICS 384, 391 (2010).

223. *See* TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 81 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) (distinguishing cyber exploitations from cyber attacks).

224. *See id.* at 151–52 (discussing the capability for multiple simultaneous functions by individual payloads and the role of command and control arrangements in determining payload functions).

225. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1 (reporting that part of the Stuxnet worm apparently mapped operations and created the equivalent of "an electrical blueprint of the Natanz plant," since efforts to seize control of the Iranian centrifuges would fail unless "every circuit was understood").

226. *See* Ellen Nakashima, Greg Miller & Julie Tate, *U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*, WASH. POST (June 19, 2012), http://articles.washingtonpost.com/2012-06-19/world/35460741_1_stuxnet-computer-virus-malware.

227. *Id.*

multiple other functions, including "wiping out a computer's hard drive."[228]

The precise nature of a hostile cyber action may thus defy easy categorization. For this reason, treating cyber acts that are designed to exploit information as fundamentally different from cyber acts that are designed to disrupt, destroy, or manipulate information (with resulting physical damage) may be difficult and inappropriate.

While the features of conventional weapon systems are physical and their use can be compared on the basis of both physical attributes and effects, the features of cyber weapons are informational and are thus harder to characterize, quantify, and distinguish from each other. This compounds the danger of imposing the IHL framework on diverse acts in cyberspace based on artificial, simplistic, or technologically ill-founded distinctions.

IV. INFORMATION AS A TARGET: PROBLEMS OF MANIPULATION AND THE CHALLENGES OF CONTENT AND USERS

Many cyber attack scenarios depict relatively simplistic efforts by states to manipulate data in cyberspace in such a way that a few mouse clicks or a few strokes on a keyboard directly and immediately cause catastrophic damage to various physical structures of an adversary (such as power plants, transportation hubs, dams, etc.).[229] If the resulting damages are sufficiently severe, a writer applying a purely consequentialist approach is likely to conclude that the IHL framework applies to such destructive hypothetical cyber actions. This simplistic cause-and-effect analysis is likely, however, to overlook critical issues associated with the content of information, the different layers of cyberspace, and the different users of information (particularly humans) in cyberspace.

A. *Information Manipulation or Exploitation? The Problem of Content and Economic Targets*

A nation's critical infrastructure includes vital economic components, including key commercial facilities, critical manufacturing sectors, and the banking and finance sectors.[230] As

---

228. Nicole Perlroth, *Researchers Find Clues in Malware*, N.Y. TIMES, May 31, 2012, at B1.

229. *See Cyber-Warfare: Hype and Fear*, THE ECONOMIST (Dec. 8, 2012), http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may (noting that, regardless of overstated vulnerabilities to cyber attack, "[t]he nightmares are of mouseclicks exploding fuel refineries, frying power grids or blinding air-traffic controllers").

230. *See* 42 U.S.C. § 5195c(e) (2006) (defining *critical infrastructure* as "systems and assets, whether physical or virtual, so vital to the United States that the

discussed above, attacks with conventional weapons on critical infrastructure, particularly economic targets, have generated considerable controversy in recent years and have sharpened the debate among governments, scholars, and nongovernmental organizations about what constitutes a legitimate military objective for targeting purposes under the IHL framework.

Concerns about using conventional weapons to attack economic targets are greatly increased by fears about compliance with the principle of proportionality. The dual-use nature of most economic targets and the civilian facilities and personnel that are likely to surround them may often mean that attacks on such targets with conventional weapons will present a high risk of excessive damage to the civilian population.

There may also be serious, practical, and nonlegal concerns related to using conventional weapons to attack financial institutions. Although dropping a bomb on a bank, stock exchange, or other financial institution may damage physical structures, it may have little effect on accounts and many other financial assets. Similarly, bombs dropped on individual physical targets may be ineffective in disrupting larger financial networks.

On the other hand, a hostile cyber act against information in financial institutions or networks themselves could achieve the previously elusive goals of destroying, or removing, key financial assets or disrupting critical financial networks. As noted, military planners may assign a high priority to destroying or disrupting key economic targets of an adversary and will continue to consider the advantages of using cyber capabilities against economic targets in future conflicts. New cyber espionage tools that can help to identify, penetrate, and survey the most lucrative economic targets will increase the likelihood that these targets will be attacked.

Notwithstanding the advantages that cyber capabilities may offer over conventional weapons when used against economic targets, their use against banks and other financial institutions remains controversial. As suggested by one senior U.S. military leader, "[I]t is difficult for me to conceive of an instance where it would be appropriate to attack a bank or a financial institution, unless perhaps it was being used solely to support enemy military operations." [231]

---

incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"); *see also Financial Services Sector: Sector Overview*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/financial-services-sector (last visited Dec. 15, 2013) (stating that "[t]he Financial Services Sector represents a vital component of our nation's critical infrastructure").

231. *See* Advance Questions for Lieutenant General Keith Alexander, Nominee for Commander, U.S. Cyber Command: Before the S. Armed Services Comm., 111th Cong. 13 (Apr. 15, 2010), *available at* http://epic.org/Alexander_04-15-10.pdf (statements of Lieutenant General Keith Alexander).

There may be a variety of concerns related to the use of cyber capabilities against financial institutions, including the possibility of far-reaching, unwanted repercussions.[232] Yet many of these concerns are based more on practical, political, or economic factors than they are on legal considerations. In this regard, planners may fail to consider the possibility that some economic targets have both military and civilian uses and may thus legitimately be subject to attack under the IHL framework.[233]

As cybercrime statistics reflect, hostile cyber actions against businesses and financial institutions routinely involve the exploitation of valuable information.[234] When intellectual property, proprietary information, bank and credit card account information, other diverse forms of financial information, or various financial assets in a digitalized form are removed or otherwise made inaccessible by a hostile cyber act, consequences alone cannot be the appropriate lens of analysis for IHL purposes.

The very nature of a hostile cyber act against an economic target makes it far more likely that the act will constitute an economic, property, or security crime under a state's domestic law than an act of violence governed by the IHL regime or an armed attack for purposes of the *jus ad bellum*.[235] Hostile, state-sponsored cyber acts against economic targets may in fact be indistinguishable from increasingly common acts of cyber fraud, larceny, or espionage. Even the characterization of the cyber act itself is problematic, since the exploitation of valuable data (through its theft and removal) may be impossible to meaningfully distinguish from the manipulation or destruction of that data.

Extending the IHL regime to encompass diverse acts of information exploitation, which are typically treated as criminal acts under the domestic laws of states, raises serious concerns about expanding the scope of modern armed conflicts into the already crowded domains of conventional criminal activities and cybercrime. It further risks undermining the viability of the IHL regime itself by transforming a multitude of economic crimes into attacks and acts of violence.

Serious questions are raised by any approach that, by focusing exclusively on economic damages, equates cyber acts involving the removal of valuable financial data with attacks under the IHL regime

---

232. *See supra* text accompanying notes 163, 165–67 (regarding the "unwritten international taboo" against cyber targeting of banking systems).

233. *See* Dunlap, *supra* note 109, at 89–90 (observing in this regard that "cyber strategists need to distinguish prudent targeting from legal mandates").

234. *See, e.g.*, Rogin, *supra* note 183 (noting that "U.S. companies lose about $250 billion per year through intellectual property theft" alone).

235. As discussed above, this point is consistent with state practice, which continues to reject the application of the cyberwar model to numerous, diverse, and hostile cyber actions that occur on a daily basis against economic targets worldwide.

(or armed attacks for the *jus ad bellum*). While economic damages may result from conventional, physical attacks, purely financial losses linked to a hostile cyber act are a poor substitute for the human suffering caused by acts of violence under the *jus in bello*. Such losses by themselves are in fact far removed from the violent deaths, injuries, and destruction that gave rise to the IHL regime itself.

Nonetheless, since financial harm represents a form of injury, some writers applying a consequentialist approach (thus interpreting or explaining the term violence as relating primarily to effects and not to acts of physical force) conclude that a hostile cyber act that causes serious economic damage, including the loss of stocks and the loss of money in bank accounts, may qualify as an act of violence for purposes of the IHL framework.[236] However, ignoring the nature of the underlying cyber act here is highly problematic.

Financial damages caused by hostile cyber acts may indeed be significant. Yet they are identical to the monetary losses associated with diminished bank accounts, 401k plans, stock portfolios, corporate assets, and other financial interests caused by a wide variety of actions, including many common, unfriendly actions taken by states far removed from armed conflict. Governments take money from private and foreign-owned entities through all manners of fiscal, regulatory, and administrative mechanisms. They can do this directly, by debiting accounts, freezing access to funds, seizing financial assets, and taking other actions executed through electronic transfers or other digital means. Many of these actions, if taken against foreign interests without their authorization, may be difficult to distinguish from various hostile cyber acts against the same economic targets.

A conclusive characterization of the effects of cyber actions against many economic targets is further clouded by the fundamental problem of what constitutes the "content" of information, especially when financial and proprietary interests can themselves be transmitted and stored as sets of data. Some advocates of a consequentialist approach suggest that the "permanent loss of assets" (such as money or stock) constitutes damage or destruction for purposes of the *jus in bello* if those assets are "directly transferable into tangible property."[237] Similarly, for purposes of the *jus ad bellum*, these consequentialists argue that the "destruction of data [which is] designed to be immediately convertible into tangible

---

236. *See, e.g.*, Schmitt, *supra* note 129, at 377 (noting that "[t]o the extent that the term 'violence' is explicative, it must be considered in the sense of violent *consequences* rather than violent *acts*. Significant human physical or mental suffering is logically included in the concept of injury; permanent loss of assets, for instance money, stock, etc., directly transferable into tangible property likewise constitutes damage or destruction.").

237. *Id.*

objects, like banking data, could also be reasonably encompassed within the scope of 'armed attacks.'"[238] Taking this a step even further, these writers suggest that while characterizing data as an object of attack may be problematic, it is nonetheless appropriate if the data has "intrinsic value."[239]

The idea that phases or formulas will be found that clearly define the status of diverse types of financial and other valuable data for purposes of establishing "damages" in armed conflict is an illusory one and presents intractable questions. When exactly is valuable data "immediately transferrable" into tangible property? Are not stolen passcodes, encrypted data for accessing financial accounts, and other types of security information immediately transferrable into a tangible financial gain once they are used against economic targets? Are not personal credit card information and other data in financial records (that can be immediately used for illicit, profitable purposes) a type of data that is immediately transferrable into tangible objects? Are these and other acts that result in monetary losses, such as the cyber theft of intellectual property, proprietary information, and other varied, digitalized "assets," the type of damage that constitutes an act of violence or armed attack? Do not all of these forms of information arguably have intrinsic value?

The questions of when data is immediately transferable into tangible property, when data has sufficient transferable value to be declared a financial asset, and when data has intrinsic value may have as many answers as there are different types of valuable information. Yet these questions must be answered definitively in order to determine the applicability of the IHL regime if a consequentialist legal standard is applied that centers exclusively on the nature of the economic damages. Suggesting that the IHL framework applies to hostile cyber acts on this basis does not, however, involve a workable standard. The content of information, with its infinite permutations, defies facile delimitations, particularly as more and more types of valuable "property" and financial interests are being placed in a digitalized format.

Somewhat similar issues greatly complicate the application of the *jus ad bellum* to hostile cyber acts in this area. The ability of the UN Charter regime to limit the use of force would be significantly weakened if the presence of an armed attack was made to depend on defining monetary losses associated with the exploited content of targeted data, establishing the exploited content's intrinsic value, or

---

238. *See, e.g.*, Schmitt, *supra* note 44, at 589 (noting, however, that "the destruction of or damage to data, standing alone, would not rise to the level of an armed attack").

239. *See, e.g.*, Schmitt, *supra* note 123, at 96 (suggesting that "it is perhaps best to treat lightly in characterizing data as an object" while noting that "some data [has] intrinsic value," for example, "digital art").

answering related questions regarding the convertibility of financial information. Furthermore, to the extent that cyber acts against economic targets undermine financial markets or result in widespread economic dislocation or hardship, challenges are presented in distinguishing such acts from other types of unfriendly or coercive economic actions that are not viewed as illegal uses of force in the international arena.

Acts involving the unauthorized use, removal, or other exploitation of valuable data clearly represent some of the most common types of criminal activity now plaguing cyberspace. Distinguishing such common crimes from identical acts of state-sponsored hostile cyber acts may be logically difficult, unworkable in terms of legal standards, and technically impossible in light of the anonymity that characterizes information in cyberspace and the architecture of the Internet. The replication or removal of valuable economic information and other forms of cyber espionage and exploitation in this area thus continue to properly remain outside both the IHL framework and the *jus ad bellum*.

B. *Manipulating Information, Layers of Cyberspace, and Users of Information*

Articles in popular media describing hypothetical cyber attacks—in which catastrophic damages are caused by the manipulation, corruption, or destruction of data—often contain images of sinister fingers touching computer keyboards, along with pictures of explosions at oil refineries, nuclear plants, and other facilities. [240] The apparent simplicity and the direct, immediate impact of such cyber acts may be deceiving and highly unrealistic. In fact, the link between a hostile cyber action and the "resulting" damages requires a careful assessment of the targeted information (upon which targeted systems, facilities, or activities depend), its content, its users, and its location in the layers of cyberspace.

Most definitions of cyberspace focus on its technical characteristics. For example, the U.S. military defines it as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures . . . including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[241] However, for purposes of targeting, it may be more

240. For example, the cover of the July 2010 issue of the *Economist* magazine featured a pixelated mushroom cloud spreading over a city with the caption: "Cyberwar: The threat from the internet." *See Cover to* 396 THE ECONOMIST, no. 8689, July 3, 2010, *available at* http://www.economist.com/node/16481504.

241. *See* DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, JOINT PUBLICATION 1-02, at 64 (amended through Nov. 2013) (defining *cyberspace*). For a similar definition that focuses on technical characteristics, see *Cyber*

useful to look at cyberspace as not only possessing various technical characteristics but also as being composed of three separate layers: a "physical layer" (including the computers, wires, routers, and other physical infrastructure assets); a "syntactic layer" (information, programs, or networks that control information systems); and a "semantic layer" (information that is "meaningful to humans").[242]

This layered approach to cyberspace has profound implications for targeting. First, it means that attacking one layer of cyberspace does not ensure penetration or control of other levels. Second, it highlights the critical difference between the users of information—that is, information in the syntactic layer that is processed by machines and information in the semantic layer, which is used by humans. Third, it recognizes the critical significance of the human semantic layer or "cognitive dimension."

Any assessment of operations in cyberspace is incomplete without including an examination of the role played by humans who receive, evaluate, act upon, and transmit information as they work with computer systems and networks—and thus make up a part of cyberspace themselves. For this reason, a more accurate definition of this metaphorical space may be "inside and by computer networks."[243] As cyberspace policy is more carefully assessed by government authorities, the term *cyberspace* may thus be described as "the virtual environment of information and interactions between people."[244]

The human, semantic, or cognitive layer of cyberspace may present a lucrative target for hostile cyber acts. While it may be more difficult to corrupt or manipulate the information going to humans than it is to corrupt or manipulate the information used to control or instruct systems,[245] hostile cyber acts directed against the cognitive layer of cyberspace can cause grievous damages. The spectrum of such damage extends across the universe of activities, machines, and systems that rely on human operators. As noted above, attacking an enemy by making data inaccessible or by disrupting information systems may achieve limited, temporary goals. However,

---

Security and Monitoring, Homeland Security Presidential Directive 23 (HSPD23) (2008) ("[T]he interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.").

242. *See* LIBICKI, *supra* note 110, at 8–9 (discussing how cyberspace can be thought of as having "three layers").

243. *See* THOMAS RID & MARC HECKER, WAR 2.0: IRREGULAR WARFARE IN THE INFORMATION AGE 57 (2009) (discussing the origins and early conceptions of the word *cyberspace*).

244. THE WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 1 (2009).

245. *See* LIBICKI, *supra* note 110, at 23 ("[I]t is usually more difficult to corrupt information going to humans . . . than it is to corrupt information that help run information systems.").

manipulating or corrupting the content of critical information upon which enemy leaders and human operators rely may yield more serious, longer lasting damage.

The legal significance of using cyber capabilities to target the semantic layer of cyberspace is profound. Such actions inject an important, manipulated, human decision-making interruption into what might incorrectly be viewed as a purely technological chain of events flowing from a cyber act to its destructive consequences. Without this human decision-making interruption, a planned hostile cyber act may be unable to cause its intended damage. As discussed below, some type of interference in this cognitive step appears to be a key feature in the most successful and complex emerging cyber weapons.

The components and operation of the Stuxnet worm illustrate how a modern cyber weapon can be designed for multiple purposes (including the exploitation and manipulation of information) and how it can be directed against different layers of cyberspace (including the syntactic layer with its human decision-making processes). Rather than the hypothetical scenario discussed above involving a cyber attack based on a simplistic, direct, mechanical "cause-and-effect" chain of events, the Stuxnet worm represents a very different reality.

Stuxnet reportedly penetrated computer systems at Natanz, a highly secure Iranian nuclear facility, in an undetected and clandestine manner and accessed information in the targeted systems through unauthorized means.[246] Once inside, it recorded, stored, and transmitted information about the operation of the targeted control systems (an exploitation process directed at information going to both machines and humans).[247] It ultimately manipulated data going to systems that controlled the facility's centrifuges to make them operate improperly, with resulting damage (a hostile act of information manipulation against the syntactic layer of cyberspace).[248] Finally, it gave false data to the Iranian centrifuge

---

246. DAVID E. SANGER, CONFRONT AND CONCEAL 196 (2012) (describing how engineers at Natanz unwittingly used infected thumb drives and laptops that reportedly transmitted the worm into the computer system there); *see also* Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. TIMES (July 13, 2013), *available at* http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?pagewanted=all (noting how Stuxnet took advantage of several valuable "zero days" vulnerabilities, "including one in a [Microsoft] Windows font program" to enter the computer system at an Iranian nuclear facility, access information, and plant codes).

247. *See* SANGER, *supra* note 246, at 196 (describing how Stuxnet reportedly first planted "beacons" that in several months were able to "report home – complete with maps of electronic directories of the controllers, and what amounted to blueprints of how the centrifuges spinning in the basement in Natanz were connected to their electronic control systems").

248. *See id.* at xi, xv (noting how Stuxnet was reportedly designed to "strike directly" at the centrifuges and how intelligence sources suggested that "just shy of a

operators indicating that the centrifuges were operating properly when they were not (a key act of information manipulation against the cognitive layer of cyberspace), thus allowing the damage to occur and not be detected—and halted—by the operators.[249]

A piece of computer code in the Stuxnet worm that had recorded and secretly transmitted back to its masters routine operations in the Natanz nuclear facility reportedly allowed the malware to later send signals to the operators in the Natanz control room "indicating that everything downstairs was operating normally."[250] This deception of the human Iranian operators regarding the status of malfunctioning centrifuges at the Natanz nuclear facility thus played a central role in causing the damage that was ultimately attributed to Stuxnet, demonstrating a close connection between data exploitation and the destruction caused by the manipulation of the data itself.[251]

The Stuxnet incident illustrates how one hostile cyber act may actually involve an elaborate series of technical events and programmed malware actions that ultimately depend on human operators to make key, damaging decisions based on their assessment of manipulated information. For purposes of applying the IHL framework, this human decision-making step in cyber actions is highly problematic. Hostile cyber acts that manipulate data in the semantic layer (with highly damaging consequences) may simply be new technologically enhanced versions of older and legally permissible activities by states, particularly conventional acts of deception and misinformation.

In terms of the IHL framework, elaborate and diverse efforts by military forces to deceive adversaries are as old as warfare itself and have long been recognized as legitimate conduct (unless constituting acts of perfidy). For example, "[r]uses or war" were explicitly recognized as permissible under the Hague Regulations of 1907.[252] Protocol I further provides that permissible ruses of war include "acts intended to mislead an adversary to induce him to act recklessly" and

---

thousand centrifuges had come crashing to a halt inside the underground cavern at Natanz").

249. *See* Jonathan V. Last, *Bride of Stuxnet: Webcraft as Spycraft*, 17 THE WEEKLY STANDARD, no. 37, June 11, 2012, at 18–19, *available at* http://www.weeklystandard.com/articles/bride-stuxnet_646424.html?page=2 ("Once Stuxnet reached its destination, it had very precise instructions: It altered the speed of the centrifuges in such a manner as to slowly degrade the equipment and destroy the uranium they contained—all while sending false readings back to the operating console so that neither the computer nor the human supervisors would notice the damage being done.").

250. SANGER, *supra* note 246, at 175.

251. *See id.* (quoting an unnamed U.S. official as saying that the ability of Stuxnet to deceive Iranian operators regarding the ongoing malfunction of the centrifuges "may have been the most brilliant part of the code").

252. Hague Convention (IV) Respecting the Laws and Customs of War on Land, Annex (Regulations), *supra* note 120, at art. 24.

"the use of camouflage, decoys, mock operations and misinformation."[253] Cyber capabilities will increase opportunities for practicing ruses of war and other acts of deception, but since the deception of humans with misinformation—however it is introduced—is explicitly permitted by the IHL framework, it is inappropriate to classify such cyber acts of deception as attacks and acts of violence.[254]

Attempts by states to use information to promote their views and influence the actions of other states and those states' populations are common and even a fundamental part of international relations.[255] The transmission of unwelcome information (by means of radio, television, and the Internet) is not, however, the equivalent of an armed attack for purposes of the *jus ad bellum* but again is more likely to resemble other nonphysical techniques of coercion (such as economic measures), which are more appropriately considered in the context of illegal acts of intervention.[256]

Many common techniques practiced by states in the fields of diplomacy, arms control, and security policy depend to a significant degree on the use of misinformation and related measures to affect the psychological disposition of their adversaries.[257] Because of their nature and regardless of their effects, such unfriendly psychological and ideological actions standing alone cannot be viewed as illegal

---

253. *See* Protocol I, *supra* note 22, at art. 37(2) (providing that "[r]uses of war are not prohibited" if they "infringe no rule of international law applicable in armed conflict and . . . are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law").

254. *See, e.g.*, Knut Dörmann, *Computer Network Attack and International Humanitarian Law*, CAMBRIDGE R. INT'L AFF. ¶ 24 (May 19, 2001), *available at* http://www.icrc.org/eng/resources/documents/article/other/5p2alj.htm (noting that "[c]omputer data creates new opportunities for practising [sic] ruses of war" and that "parties to a conflict will be tempted to plant misinformation deliberately with a view to confuse the adversary. Such misinformation about one's own military plans is perfectly lawful and is no different in principle to any other vehicle for misinformation.").

255. LEIGH ARMISTEAD, INFORMATION OPERATIONS: WARFARE AND THE HARD REALITY OF SOFT POWER 9 (2004) (arguing that "information, as an element of power, is the most fungible and useful force at all political levels, including the systemic structure of international relations in the post-Cold War era").

256. *See* Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 25/2625 (XXV), Annex, U.N. GAOR, 25th Sess., U.N. Doc. A/RES/25/2625, at 123 (Oct. 24, 1970) ("No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.").

257. *See generally* ROBERT JERVIS, RICHARD NED LEBOW & JANICE GROSS STEIN, PSYCHOLOGY AND DETERRENCE (1989) (discussing the underlying assumptions that often form the foundation for deterrence strategy).

uses of force under international law, even from a consequentialist perspective.[258]

U.S. Military manuals describing modern "information operations" further illustrate critical similarities (and overlaps) between many long-practiced, conventional misinformation practices and hostile cyber acts that target information going to humans.[259] The similarities are especially strong when comparing conventional military operations intended to "influence" decision makers (by inducing them to accept misinformation as truth or otherwise rely upon the content of incorrect information) with cyber acts that are intended to influence decision makers by making them rely on corrupted or manipulated data.

Cyber actions that target information used by humans and conventional information operations both involve the application of different forms of information on human decision makers as targets.[260] In this regard, U.S. national military strategy explicitly acknowledges that cyberspace provides a "link into the cognitive dimension."[261]

Computer network, psychological, and deception operations are all viewed by the U.S. military as tools that can be used in combination to "influence, disrupt, corrupt, or usurp [adversarial human and automated decision making] while protecting our own."[262] Thus, through both cyber and conventional methods, information operations can take "specific psychological, electronic, or physical actions that add, modify, or remove information from the environment of various individuals or groups of decision makers."[263]

The combination of human and mechanical targets and the integrated employment of human and technological capabilities blur meaningful legal distinctions between many cyber and conventional information operations. These operations may share the same objectives and employ similar methods to manipulate or corrupt data

---

258. *See, e.g.*, Schmitt, *supra* note 44, at 577 ("[I]t is well accepted that the international law governing the use of force does not prohibit propaganda, psychological warfare, or espionage. To the extent such activities are conducted through cyber operations, they are presumptively legitimate.").

259. *See, e.g.*, U.S. DEP'T OF THE AIR FORCE, INFORMATION OPERATIONS AIR FORCE DOCTRINE DOCUMENT 3-13, at vii (amended July. 18, 2011) ("The three IO capabilities—influence operations, electronic warfare operations, and network warfare operations—while separate and distinct, when linked, can achieve operationally important IO effects.").

260. *See, e,g.*, U.S. DEP'T OF DEF. & JOINT CHIEFS OF STAFF, INFORMATION OPERATIONS JOINT PUBLICATION 3-13, at I-3 to I-9, II-9 to II-11 (2012) [hereinafter JOINT PUBLICATION 3-13] (referring to "target audiences" as an "individual or group selected for influence").

261. U.S. DEP'T OF DEF. & CHAIRMAN OF THE JOINT CHIEFS OF STAFF, THE NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS 5 (2006).

262. JOINT PUBLICATION 3-13, *supra* note 260, at GL-3.

263. *Id.* at I-6 to I-8.

used by an adversary's human decision makers, often with damaging consequences for that adversary.

In this context, cyber methodologies that significantly depend on the deception of human decision makers must be carefully and cautiously assessed. To suggest that consequences alone determine the legal status of a hostile cyber act under the IHL regime when the act itself is intertwined with, and fundamentally dependent on, the use of misinformation to deceive humans represents a potentially radical revision of the IHL regime. It risks a dangerous expansion of the regime beyond recognized acts of violence to encompass many conventional information operations as well as other common state activities that have political, diplomatic, or psychological objectives (and which have long been explicitly regarded as legally permissible).

Notwithstanding these concerns as they might pertain to the targeted human operators at the Natanz nuclear facility in Iran, some writers view the physical damage associated with the Stuxnet incident as meeting the threshold for attacks under the IHL framework, based solely on the resulting physical damages. [264] However, state practice cannot be invoked to support such a position, in part because the details of Stuxnet's development and deployment remain shrouded in secrecy. Nonetheless, the fact remains that states have been reluctant to treat the Stuxnet incident as anything other than a sophisticated act of sabotage—just as Iran complained that Stuxnet had made it "the target of sabotage" (and reportedly responded to Stuxnet by taking its own harmful, covert actions against American and Western interests). [265] The question thus remains whether current state practice will change or whether complex malware packages dependent on human deception and involving a chain of mechanical events interrupted by human decision making are to be routinely evaluated by states based solely on their effects without also focusing on the nature of the underlying informational act.[266]

---

264. *See, e.g.*, Michael Schmitt, *Classification of Cyber Conflict*, 17 J. CONFLICT & SEC. L. 245, 251–52 (noting that "if a State was behind the 2010 'Stuxnet' attack . . . it would meet this threshold [attacks satisfying the armed criterion of armed conflict] because physical damage resulted").

265. *See* Thomas Erdbrink, *Ahmadinejad: Iran's Nuclear Program Hit by Sabotage*, WASH. POST (Nov. 29, 2010, 2:23 PM), http://www.washingtonpost.com/wpdyn/content/article/2010/11/29/AR2010112903468.html (reporting on Ahmadinejad's response to suspected cyber actions against Iranian centrifuges); Thomas Joscelyn, *Stuxnet and Iran's Shadow War*, THE WEEKLEY STANDARD (June 8, 2012, 8:08 AM), http://www.weeklystandard.com/blogs/stuxnet-and-iran-s-shadow-war_646788.html (noting that Iran responded to Stuxnet through various hostile covert actions, including the attempted assassination of American and other foreign diplomats).

266. Human involvement may also make the already tenuous and complex link between the origins and results of cyber actions even more difficult to discern. *See* RID, *supra* note 124, at 3 (2012) (noting that "[i]n an act of cyber war, the actual use of force is likely to be a far more complex and mediated sequence of causes and consequences that ultimately result in violence and casualties" and that in some scenarios "the

Along similar lines, an extension of the *jus ad bellum* to cyber actions that are dependent on the dissemination of misinformation to humans would risk dramatically expanding the scope and nature of that regime, potentially extending it to encompass many areas of common state practice in diverse fields. Hostile cyber acts manipulating data used by humans may in fact be difficult to distinguish from many conventional and lawful information operations, making these acts highly problematic substitutes for armed attacks under the UN Charter.

V. CONCLUSION

The unfriendly use of information by states, particularly in wartime, is as old as states themselves.[267] Modern variants, in the form of unfriendly cyber acts, are now an unwelcome but common feature of international relations. While it has long been apparent that hostile cyber acts are capable of causing great damage, to this point in history, damages alone have not been determinative of the legal status of these acts. From the physical destruction apparently caused by a logic bomb in the control system of a Siberian pipeline in the 1980s, to the widespread disruption of computer systems in Estonia in 2007, to damaged centrifuges in an Iranian nuclear facility in 2011, states have shown a consistent unwillingness to impose the armed conflict legal model or the *jus ad bellum* on hostile cyber acts standing alone.

This legally significant, widespread, and consistent state practice rejecting the cyber war model (by not actually applying IHL rules or the *jus ad bellum* to cyber acts by themselves) stands in stark contrast to much popular wisdom and the approaches of many commentators.[268] In part, this state practice reflects the political and strategic reality that hostile cyber acts are by themselves not well suited for use as instruments of armed conflict or typical armed attacks.[269] They are instead better described as "merely sophisticated

---

causal chain that links somebody pushing a button to somebody else being hurt is mediated, delayed, and permeated by chance and friction").

267. *See generally* PHILIP M. TAYLOR, MUNITIONS OF THE MIND: WAR PROPAGANDA FROM THE ANCIENT WORLD TO THE NUCLEAR AGE (1990).

268. *See, e.g., Cyber-Warfare: Hype and Fear*, *supra* note 229 (noting that "[p]olitical and military leaders miss no chance to declare that cyberwar is already upon us").

269. Thomas Rid commented that

> [t]o count as an armed attack, a computer breach would need to be violent. If it can't hurt or kill, it can't be war. An act of cyberwar would also need to be instrumental. In a military confrontation, one party generally uses force to compel the other party to do something they would otherwise not do. Finally, it would need to be political, in the sense that one opponent says, 'If you don't do X, we'll strike you . . . . No past cyberattack meets these criteria.

versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage."[270] As hostile cyber acts remain by themselves unlikely instruments of war and are relegated to other categories of unfriendly state behavior that do not involve the use of armed force, they have justifiably also remained outside the scope of the IHL framework and the *jus ad bellum*.

While the debate about the applicability of international legal models to hostile cyber acts continues, incidents of domestic and transnational cybercrime continue to multiply as national legal systems attempt to respond to this clearly growing threat. For this reason, it has been suggested that the crime or law enforcement model can be described as the best "default" position for considering unfriendly acts in cyberspace.[271]

As discussed above, the growing threat posed by cybercrime has been accompanied by an increasing willingness on the part of some states to sponsor or engage in various acts of cyber espionage, sabotage, and subversion (which in many cases may be indistinguishable from acts of cybercrime). Yet to this point, states have clearly resisted treating such hostile cyber acts as constituting "cyberwar" and have not invoked the IHL framework and the *jus ad bellum* as the appropriate legal models to actually govern any of them standing alone. At the same time, it is also clear that great risks accompany any effort to expand the IHL framework to include all manner of unfriendly state actions, thereby undermining both the *jus in bello* and the international legal prohibition on the use of force.

Hostile cyber acts clearly pose a threat to modern societies, particularly as the damaging effects of those acts have the potential to cascade through governments, military forces, industries, and national infrastructures that are becoming increasingly interconnected and fundamentally dependent on computer systems and networks. [272] Legal assessments of these events based on

---

See Thomas Rid, *End This Phony Cyberwar*, 219 NEW SCIENTIST, no. 2933, Sept. 7, 2013, at 26, *available at* http://www.slate.com/articles/health_and_science/new_scientist/2013/09/cyberwar_and_cyberattacks_it_s_really_espionage_subversion_or_sabotage.html.

270. *See* Rid, *supra* note 12, at 6 (questioning whether the "Cassandras of cyber warfare [are] on the right side of history" and noting that "[c]yber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future.").

271. *See* Dunlap, *supra* note 109, at 84 ("All things being equal, cyber strategists should default to the law enforcement modality. This makes practical sense, because many experts see cyber crime (as opposed to cyberwar) as the most serious and most common threat in the cyber domain. 'Crime,' incidentally, could include acts at the behest of a nation-state, such as cyber espionage targeting a government or industry.").

272. *See* Little, *supra* note 165, at 111 (discussing the interdependent nature of modern national infrastructures and how this interdependency problem is "further compounded by the extensive linkage of physical infrastructure with information technology systems. Communication and information technologies . . . are already

damages alone, however, neglect the importance of the underlying acts and the problems posed by information itself. Fundamental legal concepts in physical domains are linked to the physical properties of physical forces and objects, giving concepts and phrases like "territory," "attribution," "invasion," "armed force," and "acts of violence" their full meaning.

While establishing the origins of actions and finding direct connections between causes and effects in physical domains is not always easy, these issues are nonetheless explained by physical phenomena and are subject to physical rules governing space, physics, chemistry, and so forth. The domain of information, however, is fundamentally different. It consists of different layers and dimensions, as well as infinite actors and constructs. It is a domain in which identities, human cognitive functions, data, and mechanical processes may be blurred. Content problems impede meaningful classification of many cyber acts, while the pervasive problem of data exploitation further complicates attempts to establish legal thresholds, distinguish cyber acts, and define damages. For these and the other reasons set forth in this Article, the IHL regime and the *jus ad bellum* will generally not be applied to cyber events standing alone and states will continue to be reluctant to transfer the application of these frameworks from the physical to the informational.

It is not difficult to find serious, inherent challenges confronting other attempts to regulate information as a conventional weapon that reflect the four key problem areas examined in this Article. In particular, attempts to regulate information as a weapon in arms control regimes offer further compelling evidence of the fundamental, vexing, and legally significant differences between the physical and the informational.

Although a detailed examination of arms control regimes lies beyond the scope of this Article, it is clear that information makes conventional versions of such regimes highly problematic vehicles for regulating cyber weapons and conflicts in cyberspace. The origin and attribution problems of information that challenge other legal frameworks wreak havoc in arms control regimes, undermining not only monitoring and verification processes but also complementary theories of deterrence.[273] While the anonymity of information and

---

affecting infrastructure system design, construction, maintenance, operations, and control, and more change appears inevitable.").

273. *See* Lynn, *supra* note 17, at 100 ("Traditional arms control regimes would likely fail to deter cyberattacks because of the challenges of attribution, which make verification of compliance almost impossible."); John B. Sheldon, *The Case Against Cyber Arms Control*, WORLD POLITICS REVIEW (Dec. 9, 2010), http://www.worldpoliticsreview.com/articles/7273/the-case-against-cyber-arms-control ("Yet just as the problem of attribution makes it difficult to identify culprit and motive, so the anonymity of cyberspace means that any cyber arms limitation treaty will lack the crucial 'trust but verify' component.").

cyber actions presents severe challenges to many forms of legal regulation, it is a particularly destabilizing factor for arms control regimes (that depend on verification of the performance of commitments) or for any other regimes in which the participants hope to "instill and enforce behavioral norms."[274]

The unlimited availability of information and the ubiquity of information-related technologies present further foundational challenges to arms control regimes. Any attempt to define the subject matter of a cyber arms control regime must first deal with the reality that individual computers cannot "reasonably be treated as analogous to conventional weapons."[275] The availability of harmful information also means that a vast number of actors are potentially implicated in any effort to create a cyber arms control regime, in contrast to the small number of actors playing key roles in the most significant arms control agreements to date—particularly those involving nuclear weapons and other arms control initiatives during the Cold War.[276]

The widely dispersed availability of information resources will also force any group of states attempting to fashion an arms control regime to deal with another reality of information weapons: that in contrast to other military technologies such as nuclear weapons, "the private sector has essentially unlimited access to most of the technology that underlies cyberattack weapons."[277] This means that not only is the scope of the destructive uses of these weapons spread over a much wider range but also that "an extraordinary degree of intrusiveness would be required to impose controls on the private acquisition and use of cyber weapons."[278]

The designers of computer programs with possible military applications, in both the government and private sectors, must also deal with the uniquely replicable nature of information and cyber weapons. This means that subjecting such computer programs to inspection may result in the immediate loss of those information

---

274. *See Appendix A to* CYBERATTACK WORKSHOP PROCEEDINGS, *supra* note 76, at 345, 362 (noting how "the inherent anonymity of cyberattacks" makes it "difficult to hold violators of any agreement accountable" and that "behavioral norms are generally much harder to instill and enforce in an environment in which actors can act anonymously").

275. Abraham D. Sofaer, David Clark & Whitfield Diffie, *Cyber Security and International Agreements*, in CYBERATTACK WORKSHOP PROCEEDINGS, *supra* note 76, at 179, 192.

276. *See* Patrick M. Morgan, *Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm*, in CYBERATTACK WORKSHOP PROCEEDINGS, *supra* note 76, at 74 (noting that "while Cold War arms control sometimes involved numerous actors, fundamentally it was the work of a small number . . . . [A]nd some important steps could be taken unilaterally. Sustaining and stabilizing security in cyberspace will likely involve a great many more actors.").

277. *Appendix A*, *supra* note 274, at 361.

278. *Id.*

packages to adversaries and the proliferation of the weapon that is the focus of regulation.

Looming over all attempts at cyber arms control, even those involving limited attempts to restrict attacks to protect certain components of a nation's critical national infrastructure, are the intractable problems associated with distinguishing various types of unauthorized access to information. As discussed above, achieving a meaningful degree of legal precision in defining and distinguishing different types of hostile cyber acts may be extraordinarily difficult, and placing limitations on one type of action may be impossible to separate from restrictions on other actions widely accepted as lawful. [279] Yet it seems unavoidable that proposed agreements limiting acts of cyber war would nonetheless be required to distinguish hostile cyber acts that merely constitute unauthorized access to systems, temporary disruptions in those systems, and exploitation of resident information from other prohibited acts of data manipulation and destruction.

Finally, attempts to create cyber arms control agreements or precursor "codes of conduct" continue to confront a central challenge posed by information: its content. For example, beginning in 1998, Russia launched a cyber arms control initiative at the UN General Assembly (fashioned as an "International Code of Conduct") with a troublesome content-related focus, containing prohibitions on "information terrorism" as well as new "information security" concepts that essentially gave unwelcome words the status of weapons.[280]

Russian cyber arms control and information security proposals continue to focus on a state's territorial sovereignty and control over its own information resources and space, asserting that "policy authority for Internet-related public issues is the sovereign right of States." [281] These proposals further highlight the difficulties in defining what constitutes "harmful information." They also leave the

---

279. *See id.* (noting that "from the target's perspective, it may be difficult or impossible to distinguish between a cyber operation intended for attack and one intended for exploitation. Restrictions on cyberattack will almost certainly restrict cyber exploitation to a large degree, and nations—including the United States—may well be loath to surrender even in principle any such capability for gaining intelligence.").

280. *See* Tom Gjelten, *Shadow Wars: Debating Cyber 'Disarmament,'* 173 WORLD AFF., no. 4, (2010), at 33–34, *available at* http://www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament (noting that these efforts are not unlike earlier efforts by Soviet diplomats to criminalize what they referred to as "ideological aggression").

281. *See* Permanent Rep. of China, Permanent Rep. of the Russian Federation, Permanent Rep. of Tajikistan, Permanent Rep. of Uzbekistan, Annex to the Letter dated Sept. 12, 2011 from the Permanent Reps. of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, at 3, U.N. Doc. A/66/359 (Sept. 14, 2011).

status of many information activities, such as social networking through Facebook and Twitter, uncertain, based on the stated need to "prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States."[282]

It is thus not surprising that efforts to regulate the content of information under the guise of cyber arms control have highlighted how "[p]rofound differences exist among potential member states to a cyber security agreement on the privacy and human rights to be accorded users."[283] Such efforts also focus attention on inherent conflicts between state sovereignty, censorship, and the freedom of the Internet.[284]

Dangers and dilemmas clearly confront efforts to broadly impose legal regimes on information in the same manner as they apply to physical weapons and targets in the physical world, even if destructive physical consequences are involved. In spite of this, it is suggested or simply assumed that international law—particularly the IHL framework—should be used to fill perceived legal gaps in cyberspace as states compete and clash in that realm, just as those rules govern conduct in the physical world.[285] This approach corresponds with the view that conflict in cyberspace generally implicates international legal issues, rather than political, policy, or technology issues that are outside the realm of laws governing armed conflict and the use of armed force.

In an effort to affirm that law and order has been successfully imposed on cyberspace, the U.S. government has declared that "the digital world is no longer a lawless frontier."[286] However true this

---

282. *See id.* at 3–4 (pledging participating states "to cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks, and in curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment").

283. *See* Sofaer, *supra* note 275, at 194–95 (noting that "[t]he U.S. and other democratic societies are justifiably concerned that cyber system regulation—and indeed some measures that strengthen cyber security—may also result in reducing the privacy and human rights of users").

284. *See* John Markoff & Andrew E. Kramer, *U.S. and Russia Differ on a Treaty for Cyberspace*, N.Y. TIMES (June 28, 2009), *available at* http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all ("Any agreement on cyberspace presents special difficulties because the matter touches on issues like censorship of the Internet, sovereignty and rogue actors who might not be subject to a treaty.").

285. *See* DOD CYBERSPACE POLICY REPORT, *supra* note 5, at 1 (noting that "[a]s with all of the activities that DoD pursues in the physical world, cyberspace operations are . . . governed by all applicable domestic and international legal frameworks, including . . . the law of armed conflict").

286. *See* Barack Obama, *Introduction* to INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 48 ("The digital world is no longer a lawless frontier, nor the province of a small elite. It is a place where the norms of responsible, just and peaceful conduct among states and people have begun to take hold.").

statement may be regarding the reach of domestic law into cyberspace, international legal phantoms continue to abound there and must be recognized for what they are: challenging informational issues that are connected, in complex ways, to the physical world but that should generally continue to lie outside the scope of the IHL regime and the *jus ad bellum*.