Cyber Weapons and International Stability:
New Destabilization Threats Require New Security Doctrines

Guy-Philippe Goldstein

Though cyberspace is a domain of strategic importance, cyber weapons have not yet been associated with publicly well-enunciated doctrines of use comparable to that of the nuclear age. Taking two very different approaches from the strategic literature—Jervis' security dilemma and Zagare & Kilgoure's perfect deterrence model—cyber weapons are demonstrated in both cases to induce a higher level of international instability. In particular, instability is favored by the attribution issue and the lack of clear thresholds. The outline of a cyber defense doctrine, focusing on the two mentioned informational issues, is then suggested.

Keywords: cyber weapons, deterrence, doctrine, security dilemma, perfect deterrence, attribution, thresholds, escalation

In 2013 cyberspace is a domain of strategic importance.[1] The threat of cyber attacks has been placed at the top of the list of national security risks in the "Intelligence Community Worldwide Threat Assessment of 2013,"[2] and computer network warfare is one of the only military areas in both the US and in NATO countries that is expected to grow.[3] Beginning in 2009, the United States Cyber Command, for example, was established as a unified command under the United States Strategic Command. As was stated quasi-officially by the *Wall Street Journal* in June 2011, computer sabotage that is generated in another country is sometimes considered

Guy-Philippe Goldstein MBA, HEC (France), is the author of *Babel Minute Zero*, a bestseller about international cyber warfare.

by the Pentagon as an act of war. In that sense, since the effects of cyber weaponry could be substantially vast, key decisions require direct approval from the US President, as they "should be unleashed only on the direct orders of the commander in chief."[4]

There is, however, no doctrine of use that is as clearly communicated as the doctrine of nuclear deterrence. First, many rules remain secretive and strictly in the realm of the highest echelon of the executive powers. Second, the domain itself is not clearly defined: it may be a in the war fighting domain,[5] or not.[6] Is cyberspace critical only because it is conducive to military assurance?[7] Or is it critical in its own right due to the increasing value of the data stored and protected in cyberspace? Finally, the development of a doctrine takes time and historical precedents. Though concepts of nuclear deterrence began emerging in 1946 following the works of Brodie,[8] Mutually Assured Destruction (MAD) did not come to the forefront before the late 1950s.[9] In the USSR, the nuclear strategy's "learning curve" was even less advanced.[10] Certainly, the field of cyber studies is still relatively young, and cyber weaponry in itself is constantly evolving in scale and scope.

The lack of a doctrine poses a significant problem because without the proper management framework—or doctrine of use in international relations—the introduction of any untested and disruptive technologies has the potential to yield unexpected consequences. This is particularly true in the business of war. To rely solely on technological solutions without the context of a doctrine does not guarantee the preservation of the status quo. Stability during the Cold War was not assured by defensive techniques, such as efficient anti-ballistic missiles systems. Not only were these technological solutions elusive, but they were also not desirable in the preservation of the balance of terror at the heart of the MAD doctrine. Both conclusions led to the signing of the Anti Ballistic Missile (ABM) Treaty of 1972.[11]

That does not preclude the necessity of developing specific technologies, such as Submarine-Launched Ballistic Missiles (SLBM) that guarantee a capable and survivable second strike force, but they should espouse the logic of a doctrine in order to reinforce it. This is particularly true for cyberspace, whose nature and risks should indicate the necessity of such an effort. Although the topic is still relatively new, it is not an emerging issue anymore. More than 15 years have passed since the 1997 US Eligible

Receiver exercise, which triggered the first real concerns at the federal level with regard to cyber warfare.[12] In addition, the past five years were marked by several "cyber" episodes in international relations, from the Russian-Estonian cyber guerilla wars of 2007[13] to the 2012 foreign attacks against Saudi Arabia's Aramco, possibly originating from Iran.[14] Sufficient examples of recent years can supply the first guidelines on these issues and doctrines. Moreover, the field can be approached by some of the more classical legal and political frameworks. Though attention must be paid to the specificities of the domain, there are many examples that could be a baseline for the establishment of such doctrine. A recent study that could be used for the writing of such doctrine is the *Tallinn Manual on International Law Applicable to Cyber Warfare*, which managed to apply legal precedents to cyber warfare situations.[15] Following this example, the article will apply frameworks from the "classical" strategic literature in a more formal way to assess the risks cyber weapons pose to international stability and also identify the very core issues of cyber defense that must be addressed by future doctrines.

The Nature and Current Risks of Cyberspace

The Nature of Cyberspace

The definition of cyberspace has been debated extensively. The focus was usually given to the technological components (e.g., electromagnetic spectrum, information-communication technologies, and so on).[16] In this article I suggest a complementary view that asserts cyberspace is currently the name for all information systems that are based on digital data. An analog electro-magnetic radio, for example, is not considered a part of cyberspace as it does not know how to "speak digitally." A DNA computer, however, is conversant in digital data and is therefore a part of cyberspace, as is an electro-magnetic tape, which is encoded in digital data even though it is played in an analog tape recorder.

Digital information is the language humans have created to communicate with machines, which dates back to the Industrial Revolution and the invention of the Jacquard loom (1801), when the rising complexity of new machines required the creation of such a language. It took nearly two centuries for the language to spread among other machines, especially after the inventions of Turing machine computers and the internet protocol. By nature, this language consists of three components: hardware (including telecommunication equipment), software (including data exchange protocols), and "brainware," the human component that takes part of the data transmission by constituting very vulnerable interception points[17] and by writing code. Some of the most dangerous weapons in cyberspace today are, in fact, the codes produced by talented hackers. Functionally, cyberspace can be split into two: the physical support that materially affects communication and calculation, and the semantic domain that transforms physical support actions into data or instructions, providing them with meaning and controlling its own physical support.

This simplified description of cyberspace explains the current urgency to define the conditions for cyber defense and sheds light on the most critical pain points in cyberspace.

First, the distinction between digital and analog data makes clear why cyber warfare has become a strategic topic only in recent years. Although computers have been in use since the end of World War II, in 1986, digital data comprised only 0.6 percent of global data for storage, communications, and broadcasting, increasing to 24 percent in 2000. It exploded in 2007, however, reaching 93 percent, while "old" analog information capabilities became noncritical.[18] By the second half of the 2000s, information systems—what is usually most critical to any institution or organism—was fully transferred into the digital format. This may explain why the number of cyber attack episodes increased in frequency and gravity over the last few years. Civilization, including warfare, has turned digital. To use the words of Marc Andreessen, "Software has eaten the world."[19]

Second, the semantic dimension highlights and reflects the heart of networked information systems. The objective of ARPAnet, the ancestor of the internet, was to "emphasize robustness and survivability, including the capability to withstand losses of large portions of the underlying networks."[20] Packet switching networks are designed to withstand material hardware degradation. In cyberspace, the most severe damages are obtained when data are corrupted and their meaning manipulated, as was evident in "Operation Orchard"[21] and Stuxnet. In both cases, a maximum effect was obtained because human controllers were manipulated by corrupted command and control systems. In addition, the corruption of the industrial controllers that set the speed of rotors in P-1 centrifuges increased the level of sabotage.[22]

Characteristics of Cyber Attacks in Brief

In ancient Greece, the term *logos* equally signified the uttered word, the sentence, the direct meaning, and the higher level of ideas expressed.[23] It was a confused but rich definition, which also led to the development of the first hackers, the sophists, who manipulated words and syntax in order to corrupt meaning. What we call cyberspace today is, essentially, a digitalized *logos*, i.e., the language designed to communicate with machines on anything from physical support through immediate semantic translation of ordering machines or humans, and to Gibson's "consensual hallucination."[24] In this digital form of *logos*, modern sophists act like *The Sorcerer's Apprentice* of Paul Dukas: the code alters the man-made environment of machines, which causes the machines to alter the physical world by believing wrong arguments or instructions. In that sense, the quality of the attack depends first and foremost on the talent of the wizards.

The flaws used by offensive cyber weapons were developed either mistakenly or purposefully during the production stage of the equipment[25] or code or during their human handling, and were then exploited for further actions. To more precisely assess the attack's impact in the physical world, cyber warriors created models to test attacks.[26] Cyber weapons can also be designed to hide their signature and origin.[27] These characteristics give an asymmetrical advantage to the attacker once a flaw (or "exploit") has been found: only the attacker knows what the exploit is and the identity of the attacker. Since cyberspace is continuously updated by software upgrades, however, the cyber physical environment changes constantly as well, which makes the potency of exploits limited and transient: searching or manufacturing exploits requires permanent efforts.

The effects of these attacks occur as soon as the machines receive the message—the code strikes at "zero day," and their range is extremely large due to the wide use of digital-speaking machines: from espionage (penetration of machines that store information) and economic sabotage (penetration or corruption of machines storing financial values or IP addresses) to physical sabotage (attacks against machines that control and command all sorts of civilian industrial processes or weapon systems ranging from the tactical to the strategic). Because "software has eaten the world" and continues to do so, there are no potential limits to what can be attacked, and these effects have a psychological component as well. While equipment that was damaged by a kinetic attack must be replaced, equipment that was harmed by a cyber attack might appear to operate properly but doubts regarding its capabilities will remain permanently.

Geopolitical Instability Induced by Cyber Weaponry

Pro-Offense and Speed

The pro-offense, rapid, and possibly large extent of the effects mentioned above and their potential characteristics creates a military technological environment that is tilting toward the rupture of the status quo. Rober Jervis' seminal analysis on the offense-defense theory stresses that the terms of the security dilemma rely on two crucial variables: "whether defensive weapons and policies can be distinguished from offensive ones, and whether the defense or the offense has the advantage."[28] Combining these two variables to create four possible worlds, Jervis states that world powers will have the greatest difficulties in maintaining the status quo in a reality where "offensive posture is not distinguishable from [the defensive] one" and where "the offense has the advantage." Here, beliefs are as powerful as technology. For example, World War I was the product of such a world, which was termed "doubly dangerous": the technologies of machine guns and railroads gave the defense an advantage,[29] but because of Bismarck's quick victories in the preceding decades, great powers believed that military technologies were still yielding an advantage to offense.[30]

The parallelism with a military environment shaped and dominated by cyber weaponry should be obvious. First, there is a widespread belief that cyber weapons give an advantage to the offense,[31] which may lie in the perceived asymmetry of information between offense and defense. By definition, the defense ignores the existence of the flaw before it materializes, but when it does, correcting it may be too late. This argument may need to be refined and further examined, as the advantage given to the offense could be limited and transient in reality, but it is immaterial to the application of Jervis' model. As with Europe following Bismarck's victories, what matters is the belief expressed by the general consensus. Second, cyber weapons cannot be monitored, as one can hardly distinguish between offensive and defensive capabilities. Dual doctrines of use, including those of defensive and offensive uses, have been drafted in China and in major Western countries.[32] Core capabilities include assets that when examined from afar can be construed for defensive or offensive use, like IT infrastructure or code writers. Currently in cyber weaponry, there are no equivalents to Salt II's "observable differences" used to single out bombers carrying long-range Air-launched Cruise Missiles (ALCMs).[33] Defensive capability development itself is hardly distinguishable from offensive capability development since it stems in large parts from Red-Team exercises.[34]

The "doubly dangerous" risks could also be exacerbated by a rapid offense, used in a first strike. Such a "bolt from the blue" attack would be so decisive it would preempt any reactions from the defender. In an initial analysis of mutual deterrence games, Zagare showed that the fewer moves there are in a game, the more harm would be made to the status quo.[35] The incentive to strike first is shared by peer powers that are at about the same level of technological development. In that case, the perception that the attack is of equal risk to both sides would lead to Schelling's "reciprocal fear of surprise attack."[36] As Schelling writes, "Military technology that puts a premium on haste in a crisis puts a premium on war itself... If the weapons can act instantaneously by the flip of a switch, a 'go' signal, and can arrive virtually without warning to do decisive damage, the outcome of the crisis depends simply on who first finds the suspense unbearable."[37]

These lines were written a few years before ARPAnet was even established. They are echoed in the writing of US Air Force officers on war in the Information Age, stating that "preemptive employment of force may become a prerequisite for success."[38]

The dynamics leading to a conflict are also exacerbated by the ongoing technological investment in R&D cyber weaponry. The impetus for further investment is fed by the branching out of cyberspace into additional domains of civilian and military life and the need to protect these new realms of cyberspace. Since defense and offense R&D capabilities are hard to distinguish, this naturally triggers an arms race. Cyberspace's internal rate of the conversion of offline processes conversion into online ones is not always controlled by the military. Different from other revolutions in military affairs that were driven by actual contests, the thrust for digitalization of the US military continued at a high pace after the collapse of the USSR.[39] This may have been the result of the manifestation of the autonomous dynamics of digital data and software as they continue to "eat" the military. In this case, it is the qualitative evolution of technology itself that can also disrupt the status quo stability. As noted by Kissinger, countries that are opposing one another live in fear that their "survival may be jeopardized by a technological breakthrough on the part of [their] opponent[s]."[40] As stated by Joynt & Corbett, the rate of change creates an "intrinsic uncertainty about advancing technologies...{as they] cannot supply the sufficient conditions for stable deterrence."[41] Indeed, as a regional example, Horowitz notes that the cyber arms race in East Asia fuels instability.[42] Finally, beyond the growing scope of cyberspace's reach, the dynamic internal competition and constant upheaval of the IT industry generates an ongoing upgrade of cyberspace itself. These enhancements also constitute the sources of new alterations in the fabric of cyberspace and, thus, can generate new flaws. Independent from the political or military competition, this factor mechanically exacerbates the arms race.

Attribution and Thresholds

In addition to the perception that the cyberspace environment is pro-offense and prone to haste and to the field's technological domain that is constantly changing, cyberspace is also characterized by the ability to wage attacks without a clear attribution or a clear identification of the thresholds at stake following the initial impact. These factors constitute additional triggers for instability.

The lack of signature (the attribution issue) gives an advantage to the offense. If attacked, the defender does not know against whom to retaliate. This impedes the defense because the defender is not able to strike a counter-blow that could stop or deter the attacker. Without a clear aggressor, the defender will also encounter difficulties in mobilizing diplomatic relations in order to organize counter-pressure. If the defender retaliates or elevates defense against the wrong party, it may actually isolate itself more or trigger international escalation.

Attribution is therefore not a trivial issue: in war games one of the very first questions asked by the player acting as the defending head of state concerns the attacker's identity.[43] To gain weight diplomatically, attribution needs to reach a high level of certainty. This is technically hard to obtain in a limited amount of time.[44] Potential aggressors can claim "plausible deniability" and neutralize the international audience, reducing the margins of maneuver for the defender. Attribution can be inferred from the international context,[45] but this would not equate producing an incontrovertible "smoking gun," which would be required for securing diplomatic and external military support, especially in the context of the intelligence failures leading to the invasion of Iraq in 2003. Similarly, the international context could be muddied. Since the 1986 "BrainVirus" infection of digitally encoded floppy disks across the world prior to the web's existence,[46] most malware infections have been global in nature. All machines that speak the digital language are vulnerable to digital infections. Though Stuxnet is said to have targeted specific nuclear enrichment installations in Iran, it was also found in India, China, Russia, and the US.[47] That makes "plausible deniability" even easier for the attacker, which can portray itself as a victim among others.

Non-recognition of thresholds also clearly undermines stability. Schelling posits the importance of thresholds to articulate the "idiom of war."[48] For thresholds to efficiently structure the dialogue in the violent atmosphere of war, they need to possess "simplicity, reconcilability and conspicuousness,"[49] for example, the crossing of a river or a mountain, or the general mobilization of an army.

The question is all the more critical because each player's calculus depends on other players' "curve of credibility"[50]—i.e., the stakes that a country has invested in a conflict from its own volition or which was forced on it by its opponent. These stakes are delimited by the above mentioned thresholds. They are positioned within a hierarchical disposition that credibly organizes the perceived modus operandi of a government. The underlying sense of proportionality is related to the above-mentioned hierarchical disposition and is also the key to credibility. This, in turn, allows the violent dialogue to be controlled. If an error was created in understanding the opponent's curve of credibility, there is de facto a perceived "imbalance of resolve"[51]—potentially leading to the conflict's spiraling. The massive retaliation policy defined in the NSC-162/2 document, for example, was noted by William Kaufman as lacking credibility, as it was "out of character for the US" to implement it.[52] On the other hand, as identified by Frank Zagare and Marc Kilgour in their work on Perfect Deterrence Theory, the credibility of nuclear deterrence lies on the preference for retaliation over backing down.[53] This preference is assured by a capable threat (especially a survivable second strike force), but also on a rational calculus of retaliation, as this rational preference establishes credibility. If a nation's core population centers were hit, and the nation can retaliate and inflict a major cost to the aggressor, there is a high probability it will do so. Higher stakes change the pay-back calculus.

In this situation, if population centers were indeed destroyed, the state can more easily mobilize internal resources by way of national cohesion and consensus around revenge response. The option of a more forceful reaction becomes credible. Early in the nuclear age, Liddell Hart noted that "victims of aggression are driven by an uncontrollable impulse to hit back regardless of the consequences" and therefore an "aggressor may hesitate to employ atomic bombs" because of the likelihood of retaliation.[54]

Herein lies another difficulty with cyber attacks: they do not easily offer simple, recognizable, and conspicuous characterization in terms of thresholds. Would difficulties in online banking lead to financial panic or an economic disaster, and at what point would this occur? If the capital state of an attacked country had suffered a blackout, how many people would die after one day? When the Northeastern region of the US was struck by the blackout of 2003 that lasted more than 52 hours, the effects were surely not negligible but were also relatively minimal.[55] The evolution of the impact does not develop in a linear model. Difficulties are compounded by lack of precedents in the use of constantly evolving weaponry. A foreign force invading another nation's airspace is considered a breach of sovereignty, but what about cyber attacks of foreign countries that repeatedly corrupt servers used by national companies? Finally, effects may be caused by indirect and psychological actions; for example, by instilling doubts on the safe use of military or industrial capabilities, cyber weapon may induce paralysis but not directly provoke it. Is it the same when the paralysis is the consequence of a direct kinetic hit?

The consequences of lack of attribution and clear thresholds on stability can be analyzed through Perfect Deterrence Theory,[56] which posits that for a threat to be deterrent, it must be capable of creating significant pain to the threatened party so that it would prefer not to suffer from it. The threat must also be credible, as the threatening party must be perceived as preferring to use the threat rather than backing down. Without signature, however, the deterrent threat is not viable anymore, as the defending party does not know against whom to retaliate, and the secret offender is not threatened. The defender may also not be credible if it threatens to hurt everything and everyone in response to attacks of unknown origins. Similarly, even if attribution is realized but the effects are hard to measure and the distinctive thresholds at risks cannot be identified, the retaliation will not be "in kind," rather either too hard or too weak.

At a macro level, it is coherent with strategic literature that asymmetry or gaps in the information available to each party would lead to conflict. Spiraling is being modeled as triggered by errors of appreciation, or as Zagare and Marc Kilgour put it, "strategic uncertainty and unanticipated response, and both may be broadly construed as mistakes traceable to an intelligence failure, bureaucratic bungling, miscalculation, or some other cognitive or information-gathering deficiency."[57] The risks of spiraling are higher if countries retaliate against attacks that aim to create false information in the opponent's system. War can also be seen as a process that resolves an information problem: how much harm can a nation do to its opponent?[58] Resolving this question establishes a hierarchy among nations, which serves as an ordered bargaining system that is understood by all. These explanations show why war is much more probable when the two countries facing each other are of the same strength rather than when they are not, in which case the outcome would be obvious.[59] Cyber warfare's modus operandi, however, is to create confusion in data. This mode of action threatens to corrupt strategic information, create uncertainty, and pose risks that would upset the status quo.

The absence of large scale demonstration of cyber attacks has been one of the factors limiting the risk of spiraling. The capability to damage this type of weaponry is not as clearly assured as that of a kinetic or a nuclear weapon. However, both the potency of the Stuxnet worm and the understanding that "software is eating the world" have left major global powers more prone to the risks of this new class of weapons. Perceptions are transforming following changes on the ground and public declarations. The psychological frames at play, according to Jervis and Perfect Deterrence Theory, become applicable to a geopolitical environment that is under stronger influence of cyber weaponry.

Conclusion: The Need for "Escalation Control" Doctrines in Cyber Defense

There are no reasons to believe that "the diplomacy of violence"[60]—a term coined by Schelling to evoke the phenomenon of warfare—is going to vanish with the immersion of our civilization into cyberspace. Similarly, during the internet bubble of the 1990s, Michael Porter demonstrated that although the internet's "new economy" may emphasize types of cost advantages over others in the search for competitive differentiation,[61] it would still not suspend the old rules of strategy. Instead, the winners would be the ones who are able to "view the Internet as a complement to, not a cannibal of, traditional ways of competing."[62] Furthermore, the "power to hurt" is fully embodied in cyberspace, but does not supersede the laws of strategy. Cyber power can be analyzed through the classical dimensions of strategy, as elucidated by John Sheldon, Michael Howard and Colin S. Gray.[63]

New technologies do not eliminate the risks of spiraling in warfare. Instead, this depends on the effects of any technology that triggers general warfare—effects such as the perception that strategic military capabilities lean towards the offense; the possibility that defensive military capabilities could also be used by the offense; the rapid mode of action that would shorten the length of the military "game"; or the perception that quick technological change has the potential to reshuffle the balance of military forces. The strength of these factors ends up affecting the threat capability and credibility of each player, and thus alters the underlying deterrence relationship between the players. Ultimately, the deterrence balance can be summed up as an informational problem: does the party accurately recognize its enemy's capabilities and those of itself? Does the party have a good sense of its intentions and red lines, and are they clear to its enemy?

On all these accounts, and especially because of the corruption of data and strategic information, cyber weapons increase the risk of informational errors whereby a crisis escalates into overall warfare. In particular, the above discussion on lack of attribution and clear thresholds explains why this risk is so well materialized with the use of cyber weapons. Furthermore, the solution for both issues is rendered even more pressing due to the nature of a game, which becomes shorter by an innately speed-of-light technology that is perceived as pro-offense. All this shows how pressing the need is for a doctrine to manage this informational crisis. Thus, a doctrine for cyber stability will not be based solely on the capabilities for reprisal, such as a demonstrable, survivable second strike force at the heart of nuclear deterrence, but just as importantly, it would also be based on the capabilities for elucidation at the strategic level. If the truth about attribution and damage assessment cannot be established, then the defending party is at risk of either conceding defeat to an unknown attacker, or of engaging in reprisals "in the dark" with a high risk of spiraling. On the other hand, if the truth is fully established in the "brainware" of the strategic decision makers—if not in the whole of the software and hardware systems of the defending nation—then at least the defender can unlock all of its other traditional options from diplomatic to strategic threats in order to credibly force the offender to back down. The parallels with the truth-seeking objectives of intelligence services should not be surprising: if in cyber, as in intelligence, "the truth shall make you free,"[64] then it is partially due to the fact that both fields operate in information domains, with one based in the digital format and the other on "secrecy."[65]

The outline of such cyber defense doctrines could resemble that of elucidation actions like counter-intelligence or police investigations, but it must be strategically led by the head of state. These investigations would be supported by strong technical capabilities and operated by state-of-the-art methodologies aimed at truth-seeking from deductive testing for attribution to systems simulation for red-lines assessment. They would also have a strong diplomatic component, leveraging some circles of very close cooperation. The establishment of the truth cannot be dictated by one center. It consists of a social process based on either the sharing of the data supporting the conclusions, carefully taking into account the constraints posed by the intelligence context, or the ability to replicate experiments.[66] In that respect, military defense doctrines in cyberspace are somewhat parallel to the disciplined, scientific approach to problem solving that has been taken recently by the management of corporations from marketing[67] to human resources.[68] To attain the highest ground in an informational domain is to reach for the truth.

Notes

[1] This article explores the strategic risks of cyber weapons and the need to develop specific doctrines for cyber defense in order to offset the risk of out-of-control crisis escalation. To detail such doctrines would go beyond the scope of the current article. The author will explore some of the doctrinal solutions to the stability problems exposed here in an upcoming article.

[2] Luis Martinez, "Intel Heads Now Fear Cyber Attack More than Terror," *ABCNews*, March 13, 2013, http://abcnews.go.com/Blotter/intel-heads-now-fear-cyber attack-terror/story?id=18719593.

[3] Despite austerity cuts, the UK's cyber security budget has been expected to grow by some £650m ($1.07bn) over the 2012-2015 period. In James Blitz, "Country Profile: UK Defences are Boosted to Fight e-Crime," *Financial Times*, June 2, 2011.

[4] David E. Sanger and Thom Shanker, "Broad Powers Seen for Obama in Cyberstrikes," *New York Times*, February 3, 2012.

5 Keith B. Alexander, "Warfighting in Cyberspace," *Joint Forces Quarterly* 46, no. 3 (2007): 58-61.

6 Martin C. Libicki, "Cyberspace is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 325-40.

7 Libicki, "Cyberspace is Not a Warfighting Domain."

8 Bernard Brodie, "The Development of Nuclear Strategy," *International Security* 2, no. 4 (1978): 65-83.

9 Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: Palgrave Macmillan, 2003), pp. 234-36.

10 Freedman, *The Evolution of Nuclear Strategy*, pp. 243-44.

11 See for example Freedman, *The Evolution of Nuclear Strategy*, p. 338.

12 See PBS interview with former Deputy Secretary of Defense John Hamre in Michael Kirk, "Cyberwar!" *PBS*, April 24, 2003, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html.

13 See BBC World Service, "Estonia Hit by 'Moscow Cyber War," *BBC News*, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm.

14 See Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, October 23, 2012.

15 Michael N. Schmitt, gen. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

16 See Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), pp. 26-28.

17 Human errors in security configurations have been also identified as "responsible for 80% of Air Force vulnerabilities," in James A. Lewis, ed., *Securing Cyberspace for the 44th Presidency* (Center for Strategic and International Studies, 2008), p. 55. The rise of social engineering and phishing attacks has accentuated the importance of the "human factor" in cyber security. - It's not a quote—it's an expression. Kevin Mandia notes, "While previous generations of attacks targeted technology such as networks and servers and exploited vulnerabilities in software, attackers have now evolved to target human inadequacies and weaknesses." Kevin Mandia, "Cyber Threats and Ongoing Efforts to Protect the Nation," *Permanent Select Committee on Intelligence, US House of Representatives*, October 4, 2011.

18 Martin Hilbert and Priscila Lopez, "The World's Technological Capacity to Store, Communicate and Compute Information," *Science* 332, no. 6025 (2011): 60-65.

19 Marc Andreessen, "Why Software is Eating the World,"*Wall Street Journal*, August 20, 2011.

20 Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen

Wolff, *A Brief History of the Internet* (The Internet Society, 2012), http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

21 See David A. Fulghum, "Why Syria's Air Defenses Failed to Detect Israelis," *Aviation Week & Space Technology*, October 3, 2007, and David A. Fulghum, "Israel Used Electronic Attack in Air Strike against Syrian Mystery Target," *Aviation Week & Space Technology*, October 8, 2007.

22 See Nicolas Falliere, Liam O Murchu ,and Eric Chien, *W32. Stuxnet Dossier* (Symantec, 2010).

23 Barbara Cassin, CNRS, "Logos et Polis: La Force du Discours," in Catherine Golliau ed., *La Sagesse Grecque* (Paris: Le Point Référence, 2011), pp. 41-43.

24 William Gibson, *Neuromancer* (New York: Ace Science Fiction, 1984).

25 See the issue of kill switch in chips in Sally Adlee, "The Hunt for the Kill Switch," *IEEE Spectrum*, May 1, 2008.

26 For example, according to David Sanger, when Israel and the US developed a "bug" to derail nuclear enrichment operations at the Natanz plant in Iran, research teams "began building replicas of Iran's P-1 centrifuges" since "the bug needed to be tested." See David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012. In particular, the Dimona complex in Israel may serve as a testing ground for cyber attacks of centrifuges—see William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

27 The issue of cyber attacks attribution is a major difficulty explored in fiction—see for example, Guy-Philippe Goldstein, *Babel Minute Zero* (Paris: Denoel, 2007—and illustrated in real life episodes such as the cyber attacks against Estonia in 2007. See Mikko Hypponen,"9thof May," *F-Secure Weblog*, February 15, 2010, http://www.f-secure.com/weblog/archives/archive-052007.html.

28 Robert Jervis, "The Security Dilemma," *World Politics* 30, no. 2 (1978), p. 187.

29 See a detailed discussion in Charles L. Glaser and Chaim Kaufmann, "What is the Offense-Defense Balance and Can We Measure It?" *International Security* 22, no. 4 (1998): 44-82.

30 Robert Jervis, "The Security Dilemma," p. 190.

31 In 2009, Gregory J. Rattray highlights the "offense dominance" in Cyberspace - see Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), pp. 253-74. Three years later, David T. Fahrenkrug from the Office of Net Assessment / Office of the Secretary of Defense, notes that "Current accepted wisdom in cyberspace is that the attacker has the decisive advantage" - in David T. Fahrenkrug, *Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy*, 4th International Conference on Cyber Conflict (Tallinn: NATO CCD COE Publications, 2012).

32 New military development programs announced in 2012 for both DARPA and the US Air Force indicate- a clear interest in offensive weaponry. See Tom Gjelten, "First Strike: US Cyber Warriors Seize the Offensive," *World Affairs*, January/February 2013; additionally, in March 2013, "General Keith Alexander, who heads the US National Security Agency and Cyber Command, told lawmakers Tuesday that the military is creating at least 13 units which would have offensive capabilities in cyberspace." in "Obama Calls China Cyber Attacks 'State Sponsored,'" *News Wires*, March 13, 2013. In France, the project for the 2013 "Livre Blanc" mentions the need for LIO, aka "Lutte Informatique Offensive" or Offensive Cyber Warfare—in Vincent Lamigeon, "Livre Blanc de la Defense: Les 5 Nouvelles Priorités Imposes à l'armée Francaise," *Challenges*, April 29, 2013.

33 See Thomas K. Longstreth and Richard A. Scribner, "Verifications of Limits on Air Launched Cruise Missiles," in Frank von Hippel and Roald Z. Sagdeev, eds., *Reversing the Arms Race: How to Achieve and Verify Deep Reductions in the Nuclear Arsenals* (New York: Gordon and Breach, 1990), p. 185

34 For a very short US overview, see Zachary Fryer-Biggs, "Building Better Cyber Red Teams," *Defense News*, June 14, 2012.

35 Frank C. Zagare, *The Dynamics of Deterrence* (Chicago: University of Chicago Press, 1987), pp. 48-56—see discussion on rules relaxation and lengthening the game.

36 See Chap. IX, "The Reciprocal Fear of Surprise Attack," in Thomas C. Schelling, *The Strategy of Conflict* (Harvard University Press, 1960).

37 Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), p. 225.

38 See David S. Fadok, Major, USAF, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis* (Maxwell Air Force Base: School of Advanced Air Power Studies, 1995), p. 49. One year earlier, John Warden stated already that "Capturing and exploiting the datasphere may well be the most important effort in many future wars." The conquest of "datasphere" is implicitly defined as a priority for military success. See Col. John A. Warden III, USAF, "Air Theory for the Twenty-first Century," in *Challenge and Response: Anticipating U.S. Military Security Concerns*, ed. Karl P. Magyar (Maxwell AFB, Ala.: Air University Press, 1994)

39 See Keith L. Shimko, *The Iraq Wars and America's Military Revolution* (New York: Cambridge University Press, 2010), p. 129.

40 Henry Kissinger, "Arms Control, Inspection and Surprise Attack," *Foreign Affairs* 38, no.4 (1960): 557-75.

41 Carey B. Joynt and Percy E. Corbett, *Theory and Reality in World Politics* (London: Macmillan Press, 1978), pp. 92-93.

42 Michael Horowitz, "Information Age Weaponry and the Future Shape of Security in East Asia," *Global Asia* 6, no. 2 (2011).

43 On the issue of US Defense officials publicly struggling with the issue of attribution, see John Markoff, David E. Sanger, and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times*, January 26, 2010; David E. Sanger and Elisabeth Bumiller, "Pentagon to Consider Cyberattacks Acts of War," *New York Times*, May 31, 2011.

44 In a recent example, after facing a simultaneous shutdown of computer networks at several major broadcasters and banks on March 20, 2013, South Korea first said that cyber attacks came from China, in Warwick Ashford, "South Korea Says Cyber Attack Came from IP Address in China," *Computer Weekly*, March 21,2013. South Korea publicly admitted a mistake the next day. See Warwick Ashford, "South Korea Admits Mistake in Linking Cyber Attacks to China," *Computer Weekly*, March 22, 2013. Three weeks later, South Korea accused North Korea. See Warwick Ashford, "South Korea Accuses North Korea of Launching Cyber Attacks," *Computer Weekly*, April 11, 2013.

45 For a thesis minimizing the "attribution problem" by analysis of the international context, see Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington D.C.: National Defense University Press, 2009), pp. 309-42.

46 Rupert Goodwins, "Ten Computer Viruses that Changed the World," *ZDNet*, August 3, 2011.

47 Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32. Stuxnet Dossier* (Symantec, 2010), p. 6 and "Chinese infections in Stuxnet 'Cyber Superweapon' Moves to China," *AFP*, September 30, 2010.

48 Schelling, *Arms and Influence*, p. 135: "Finite steps in the enlargement of a war or a change in participation. They are conventional stopping places or dividing lines. They have a legalistic quality, and they depend on precedents or analogy. They have some quality that makes them recognizable, and they are somewhat arbitrary....We don't make them or invent them, but only recognize them....Apparently, any kind of restrained conflict needs a distinctive restraint that can be recognized by both sides, conspicuous stopping places, conventions and precedents to indicate what is within bounds and what is out of bounds, ways of distinguishing new initiatives from just more of the same activity."

49 Schelling, *Arms and Influence*, p. 137.

50 See Carey B. Joynt and Percey E. Corbett, *Theory and Reality in World Politics* (Pittsburgh: University of Pittsburgh Press, 1978), pp. 94-95.

51 See Frank C. Zagare and D. Marc Kilgour, *Perfect Deterrence* (Cambridge: Cambridge Studies in International Relations, 2000), p. 301.

52 See Freedman, *The Evolution of Nuclear Strategy*, pp. 96, citing William Kaufman, *Military Policy and National Security* (Princeton University Press, 1956), p.21, 24-25.

53 Frank C. Zagare and D. Marc Kilgour, *Perfect Deterrence*, chapter 3.

54 See Freedman, *The Evolution of Nuclear Strategy*, p. 40 citing B. M. Liddell Hart, *The Revolution in Warfare* (London: Faber and Faber, 1946) pp. 85-86.

55 In New York City, during the blackout, there were significant increases in respiratory, cardiac, and other EMS calls. See Gary Kalkut, MD, MPH, "Effects of the August 2003 Blackout on the New York City Healthcare Delivery System: A Lesson for Disaster Preparedness," *Critical Care Medicine* 33, no. 1 (2005), pp. S96-S101. Reports by the press, as cited on Wikipedia, accounts for 11 indirect fatalities (http://en.wikipedia.org/wiki/Northeast_Blackout_of_2003); however, a further study indicates that "there was minimal morbidity and mortality reported that could be attributed to the event." See J. Kile, S. Skowronski, M.D. Miller, S.G. Reissman, V. Balaban, R.W. Klomp, D.B. Reissman, H.M. Mainzer, A.L. Dannenberg, "Impact of 2003 Power Outages on Public Health and Emergency Response," *Pre-hospital and Disaster Medicine* 20, no. 2 (2005): 93-97. The estimates of total costs in the United States range between $4 billion and $10 billion US dollars, or less than 0.1 % of US GDP. sSee U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* (2004), p.1.

56 See Zagare, and Kilgour, *Perfect Deterrence*.

57 Zagare and Kilgour, *Perfect Deterrence*, p. 302.

58 Put differently, if states knew the outcome of a possible war and had perfect information on each other's capabilities and resolve, they would probably avoid war. See James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995): 379-414 and Dan Reiter, "Exploring the Bargaining Model of War," *Perspective on Politics* 1, no.1 (2003): 27-43.

59 See empirical analysis in Stephen L. Quackenbush, "General Deterrence and International Conflict: Testing Perfect Deterrence Theory," *International Interactions* 36, no. 1 (2010): 1-26.

60 Schelling, *Arms and Influence*, chapter 1.

61 See Michael Porter, "Strategy and the Internet," *Harvard Business Review*, March 2001.

62 See Porter, "Strategy and the Internet."

63 John B. Sheldon, "The Dimensions of Strategy for Conceptualizing Cyberpower: Laying the Foundations for Sensible Cyber Security Policy and Doctrine," presented to the panel on "Comparative Cyber Security Strategies: Theory and Practice," International Studies Association Conference, San Diego, 2012.

64 Extract from the Gospel according to St. John, initially inscribed on the CIA building's facade. See https://www.cia.gov/news-information/featured-story-archive/ohb-50th-anniversary.html.

65 See for example Michael Warner, "Wanted: A Definition of Intelligence," *Studies in Intelligence* 46, no. 3 (2002), pp. 20-21.

66 Sharing of data is a core requirement for any submission to peer reviewed journals. See for example the recommendations for *Nature*: http://www.

nature.com/authors/policies/availability.html; Evidently, in intelligence matters, sharing must balance the gain from sharing with the risks of exposure for the source—what Director of National Intelligence (DNI) James R. Clapper has referred to the need to find the "sweet spot" between sharing and protecting information. See Remarks and Q & A by Director of National Intelligence, Mr. James Clapper, 2010 Geospatial Intelligence Symposium, New Orleans, Louisiana, November 2, 2010, quoted in Richard A. Best Jr., "Intelligence Information: Need-to-Know vs. Need-to-Share," *Congressional Research Services*, June 6, 2011.

[67] See the impact of A/B Testing in management of Silicon Valley startup companies up to Google in Brian Christian, "The A/B Test: Inside the Technology That's Changing the Rules of Business," *Wired*, April 25, 2012.

[68] See Steve Lohr, "Big Data, Trying to Build Better Workers," *New York Times*, April 20, 2013.