The Journal of Strategic Studies
Vol. 35, No. 3, 401–428, June 2012

Routledge
Taylor & Francis Group

Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War

ADAM P. LIFF

Doctoral Candidate, Department of Politics, Princeton University, USA

ABSTRACT This article examines the implications of the proliferation of cyberwarfare capabilities for the character and frequency of war. Consideration of strategic logic, perceptions, and bargaining dynamics finds that the size of the effect of the proliferation of cyberwarfare capabilities on the frequency of war will probably be relatively small. This effect will not be constant across all situations; in some cases the advent of cyberwarfare capabilities may *decrease* the likelihood of war. On the other hand, the use of computer network attack as a brute force weapon will probably become increasingly frequent.

KEY WORDS: Cyber-Security, Cyber War, Strategy, Bargaining, Coercion, Deterrence, Proliferation

Once the stuff of science fiction, cyberwarfare is now a major security concern of political and military leaders around the world. Recent related, headline-grabbing events include the hostile use of cyberspace against Estonia in 2007 and between Georgia and Russia in August 2008. Beyond merely disrupting networks and information flow, cyberattacks with significantly graver consequences are also on the horizon. 'Stuxnet', a highly sophisticated malware developed specifically for cross-domain destruction of physical infrastructure, may be a harbinger of what is to come. Attacks in the cyber-domain do not only pose a threat to the security of small and relatively weak states; US political and military leaders are also concerned about the growing threat that operations in cyberspace pose to national security. Recognizing the danger that cyberattacks pose to civilian targets, President Barack Obama noted in a 2009 speech that 'our digital

ISSN 0140-2390 Print/ISSN 1743-937X Online/12/030401-28 © 2012 Taylor & Francis
http://dx.doi.org/10.1080/01402390.2012.663252

infrastructure [... is] a strategic national asset'.[1] To counter cyber threats more effectively, the US military stood up USCYBERCOM as a unified sub-division of US Strategic Command in May 2010, while the 2010 Quadrennial Defense Review calls cyberspace 'as relevant a domain for DoD [Department of Defense] activities as the naturally occurring domains of land, sea, air, and space'.[2]

Writing about the significance of the atomic bomb in his 1946 book *The Absolute Weapon*, Bernard Brodie noted, 'We know that it is not the mere existence of the weapon but rather its effects on the traditional pattern of war which will govern the adjustments which states will make in their relations with each other.'[3] He argued that atomic weapons, against which there was no defense, were a game-changing technology with significant implications for how states interact. No comparable comprehensive assessment of the impact of cyberwarfare capabilities exists.[4] Outside the slowly emerging policy literature there is limited scholarly work on the topic, leaving important theoretical questions unexamined. One fundamental question is: what will the impact of the proliferation of cyberwarfare capabilities be on the character and frequency of war in the international system?

The central objective of this article is to explore the implications of the proliferation of cyberwarfare capabilities for the character and frequency of interstate war. This article has three specific motivations: first, to promote the issue of cyberwarfare as a topic of scholarly inquiry among international relations scholars; second, to subject the assumptions and logic behind the conventional wisdom emanating into the public sphere about cyberwarfare to dispassionate analysis, particularly in the context of possible threat inflation from what some have called a nascent 'cyber-industrial complex'; third, to qualify some existing arguments about the threat posed by cyberwarfare, many of which focus almost exclusively on current vulnerabilities and are largely devoid of considerations of strategic logic, bargaining, and coercion, all of which are sine qua non for understanding how frequently and under what conditions war will occur.

[1] The White House, 'Remarks by the President on Securing Our Nation's Cyber Infrastructure', 29 May 2009, <www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/>.

[2] US Department of Defense, *Quadrennial Defense Review (QDR) Report*, Feb. 2010, 38.

[3] Bernard Brodie, 'War in the Atomic Age,' in Bernard Brodie (ed.), *The Absolute Weapon: Atomic Power and World Order* (New York: Ayer 1946), 23.

[4] In this article, cyberwarfare capabilities are defined as the capability to launch and/or defend against non-kinetic computer network attacks.

Theorizing about a kind of warfare that has not occurred necessitates a major caveat: the chief contribution of this article is theoretical and its conclusions should be treated as preliminary. It does not – and cannot – provide empirical tests.[5] It suggests and examines several hypotheses in order to try to make what we know more intelligible and challenge some of the more extreme claims about cyberwarfare. While the author believes that the logic underpinning his analysis is sound, this article is merely a first cut at a complex and evolving issue. As manifest in the major contributions to our understanding of nuclear weapons and strategy by Brodie and his contemporaries a paucity of data is not a sound rationale for neglecting a topic with possible major implications for national security. The hope is that this article will serve as a foundation for further scholarly work on the implications of the proliferation of cyberwarfare capabilities for interactions between states.

The Importance of Understanding Cyberwarfare

Despite its increasing salience to policymakers and defense planners, the issue of cyberwarfare has not caught the attention of most students of international relations. Much of the limited existing literature has emerged from US war colleges, policy-oriented research institutions, and think tanks and is often under-theorized.[6]

Some may claim that cyberwarfare is not relevant to academic security studies because 'data packets don't hold ground' and/or no one has ever died from a cyberattack. Although it may be true that a cyberattack (using known existing technologies) is unlikely to *directly* cause massive casualties, it could still serve as an effective means of political coercion or brute force.[7] At the strategic level, cyberattacks could be used as a coercive counter-value weapon to wreak havoc on

[5] The data that would be necessary for an empirical study either do not exist or are highly classified. Governments, militaries, and private corporations have strong incentives not to reveal information about attacks. Furthermore, as will become clear in the 'defining cyberwarfare' section below, there is no example of an event in the real world that can indisputably be cited as an occurrence of cyberwarfare.

[6] Notable exceptions include Gregory Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press 2001); Franklin Kramer *et al.* (eds), *Cyberpower and National Security* (Dulles, VA: Potomac Books 2009); and Kristin Lord and Travis Sharp (eds), *America's Cyber Future* (Washington, DC: CNAS June 2011). Unfortunately, these works seem to have not yet caught the attention of most academic international relations scholars.

[7] Distinct from coercive acts, which aim to extract concessions from the target, brute force measures are those in which the damage done by the attack serves as an end in itself.

networks in major financial centers or to disable or destroy critical physical infrastructure (e.g., power generators; air traffic control systems). At the tactical level, even setting aside the potential threat to ostensibly secure classified, air-gapped networks (e.g., JWICS (Joint Worldwide Intelligence Communications System) or the US military's SIPRNet or Secret Internet Protocol Router Network) used for classified intelligence transfer, cyberattacks could be used as a (kinetic or non-kinetic) brute force weapon to destroy precisely physical infrastructure or to disable or disrupt the internet-connected unclassified military and civilian networks (e.g., NIPRNet or Non-classified Internet Protocol Router Network) upon which major powers rely to project conventional military force.[8] Although the mere existence of enabling technologies by no means makes cyberwarfare inevitable, the fact that we have not yet seen a cyber-incident as shocking as Pearl Harbor or 9/11 is not a cogent justification for academics to neglect the topic.

Defining Cyberwarfare

Writings on cyberwarfare have long been plagued by major definitional problems, one consequence of which has been a lack of analytical coherence. It is especially important for theory development and the formulation of foreign policy that a clear definition be established that differentiates cyberwarfare from ostensibly cognate concepts.

The meaning of 'cyberwarfare' has become so convoluted in popular discourse that this article should preface its formal definition with an explanation of what it is not. First, the term 'cyberwarfare' applies strictly to computer network operations (CNO) whose means – if not necessarily its indirect effects – are non-kinetic.[9] Second, it does not include operations in cyberspace that constitute psychological warfare. Third, and most importantly, cyberwarfare is conceptualized as including only computer network attacks (CNA) *with direct political and/or military objectives* – namely, attacks with coercive intent and/or as a means to some strategic and/or brute force end – and computer network defense (CND). It should be emphasized that cyberwarfare

[8] Mission-critical systems rely on defense contractors and allies whose networks are far less secure than the US military and intelligence community's classified networks. More than 90 per cent of the US military's energy is generated and distributed by private companies, while more than 80 per cent of its logistics are transported by the private sector. An 'air-gapped network' is a network that is not connected to non-proprietary networks such as the world-wide web.

[9] My analysis does not consider electronic warfare or any form of kinetic (physical) attack, even those that may aim to affect command and control networks or systems, such as an anti-satellite weapon.

does not subsume those acts most frequently reported in the media as such: for example, hacking for fun, profit-driven cyber-crime, or cyber espionage and other forms of computer network exploitation (CNE), the objectives of which are neither *directly* coercive or brute force in nature.[10] Restricting the definition of cyberwarfare in this manner is necessary for theoretical and analytical clarity.

It is also important to note that 'CNA' is an umbrella category for a number of different cyberweapons, each of which has certain distinguishing features. Table 1 below provides a basic overview of CNA means that might be utilized in a cyberwar.

A good definition of cyberwarfare should (a) be informed by a model of conflict and (b) resist the urge to essentialize cyberwarfare as fundamentally distinct from more 'conventional' forms of warfare simply because it occurs in a nontraditional 'domain'. This article adopts a model of conflict that conceives of war as part of a political bargaining process between two or more actors and holds that limiting 'cyberwar' to conflict *contained completely within cyberspace* risks leading analysts to exaggerate seemingly novel and disturbing aspects of CNA (e.g., plausible deniability) and restrict their analyses to the most unlikely, and in some cases fantastical scenarios.[11] The latter approach also inappropriately excludes CNA that either indirectly damage or destroy targets in the physical world (e.g., Stuxnet) or function as a conventional force multiplier (e.g., Operation 'Orchard').[12]

This article defines cyberwarfare as a state of conflict between two or more political actors characterized by *the deliberate hostile and*

[10] 'CNA' and 'cyberattack' will be used interchangeably in this article. CNA: Actions taken through the use of computer networks to alter, disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CND: Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within information systems and computer networks. CNE: Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Adapted from: 'JP 1-02, DOD Dictionary of Military and Associated Terms.'

[11] For more on war as part of a bargaining process, see James Fearon, 'Rationalist Explanations for War', *International Organization* 49/3 (Summer 1995), 400. Any definition of cyberwarfare as a one-sided and/or single act falls short. One example is that found in Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco 2010), 6.

[12] Operation 'Orchard' refers to Israel's 2007 airstrike on an alleged Syrian nuclear reactor, which is believed to have involved a successful Israeli cyberattack that rendered Syria's air-defense network ineffective. See David A. Fulghum *et al.*, 'Israel shows electronic prowess', *Aviation Week & Space Technology*, 25 Nov. 2007.

Table 1. Types of Computer Network Attack

Type of attack	Description	Key characteristics	Possible targets	Real-world example of CNA of this type
Botnets/Distributed Denial-of-Service (DDoS) attacks	A flood of traffic from a large number of systems (some of which may have been hijacked and turned into 'bots' using malware) designed to crash or disrupt network access	Relatively low cost; not very complex; direct effects are limited to disrupting access to networks rather than cross-domain destruction	Any network (most likely Internet-connected)	Cyber exchange during 2008 war between Russia and Georgia that shut down government websites and prevented Georgians from accessing outside websites
Basic malware	A computer program that employs numerous surreptitious means (including zero-day exploits) to open up an access point, transmit data, and/or disrupt the way that target systems behave	Low cost; useful against poorly secured systems and unvigilant users	Any computer or network	Viruses, phishing scams, worms
Advanced malware	Same as above	Advanced malware able to disrupt heavily-defended systems/air-gapped networks require high level of expertise to design and implement	Critical infrastructure	Stuxnet, which is believed to have targeted (and at least partially destroyed) Iran's nuclear centrifuges[1]

(*continued*)

Table 1. (*Continued*)

Type of attack	Description	Key characteristics	Possible targets	Real-world example of CNA of this type
		Costly, both in terms of time and financial resources necessary to, *inter alia*, conduct reconnaissance, mirror the environment in the target system, introduce the malware to a non-networked system, etc. Potential to directly target and potentially physically destroy or disable specific infrastructure		

Note: [1]For an excellent technical overview of Stuxnet, see Nicholas Falliere, *et al.*, *W32.Stuxnet Dossier* (CA: Symantec Security Response 2011). For a more general discussion, see William J. Broad, *et al.*, 'Stuxnet worm used against Iran was tested in Israel', *New York Times*, 15 Jan. 2011.

cost-inducing use of CNA against an adversary's critical civilian or military infrastructure with coercive intent in order to extract political concessions, as a brute force measure against military or civilian networks in order to reduce the adversary's ability to defend itself or retaliate in kind or with conventional force, or against civilian and/or military targets in order to frame another actor for strategic purposes. This definition departs from much of the existing literature by drawing less from abstract lessons and quotations of Sunzi (Sun Tzu) and more from concrete and analytically tenable conceptualizations of war (e.g., Clausewitz).[13]

Cyberwarfare and Its Implications for Interstate War

Part 1: Implications for the Frequency of War in the International System

Journalists, analysts, policymakers, and military leaders have expressed grave concerns about the implications of the emergence of cyberwarfare capabilities for international stability. Ostensibly unique characteristics of cyberwarfare are sometimes held up to suggest implicitly or explicitly that the advent of cyberwarfare is a 'game-changer'. Four of the most frequently cited concerns are: CNA's usefulness as an asymmetric weapon; the destabilizing consequences of 'plausible deniability;' the offensive advantage resulting from the difficulty of effective CND; and the difficulty of credibly deterring cyberattacks. This section examines these claims, which are frequently made in a theoretical vacuum. Whether they are valid will depend on what one believes about the underlying strategic interactions between states. The assessment yields the following conclusions: although there is reason for concern that the proliferation of cyberwarfare capabilities may increase the frequency of war in the international system at large, its net effect will be relatively small; in most cases it is unlikely to significantly increase the expected utility of war between actors that would otherwise not fight. Furthermore, a cyberwarfare capability may paradoxically be most useful as a deterrent against conventionally superior adversaries in certain circumstances, thus *reducing* the likelihood of war. Nevertheless, CNA may be particularly expedient

[13] Clausewitz defines war as 'an act of violence intended to compel our opponent to fulfill our will;' i.e., war is political and coercive in nature. Carl von Clausewitz, *On War* (Harmondsworth, UK: Penguin 1982), 101. For another recent article that also adopts a Clausewitzian interpretation of cyberwar, see Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35/1 (Feb. 2012), 5–32, <www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939>.

as a brute force measure under circumstances in which conventional force would risk retaliation.[14]

CNA as an Asymmetric Weapon: 'The Great Equalizer?'

Hypothesis 1: CNA is an example of a low-cost, yet potentially devastating asymmetric weapon. Cyberwarfare's expediency as a kind of asymmetric warfare will increase the frequency of war by increasing the probability of war between weak and strong states that, because of sizable disparities in conventional military strength, would otherwise not fight.

Many argue that the most worrisome aspect of cyberwarfare is its low cost, which may help to level the strategic playing field among states.[15] Coupled with the weakness of existing military and civilian cyberdefenses, the idea is that relatively low barriers to entry may afford actors with weak conventional military capabilities the ability to threaten more powerful states.

Why is cyberwarfare believed to be more likely to be asymmetric than conventional warfare? Take the salient example of the US military. Much of the US's conventional military preeminence stems from its effective exploitation of advanced technology, in particular networks and information systems. However, the US dependence on computers and networks in both the military and civilian sectors, together with the US military's conventional dominance, paradoxically make it an inviting and vulnerable target for cyberattack.

US military dependence on computers, information operations, and cyberspace – not only classified networks for network-centric warfare but also unclassified military and civilian networks for precisely coordinated logistics – could be exploited in a counter-force cyberattack by conventionally inferior adversaries.[16] Meanwhile, a

[14] These conclusions differ from those of a recent article in this journal (published after this article was accepted for publication), which concludes categorically that 'cyber war will not take place'. See Rid, 'Cyber War Will Not Take Place'.

[15] The former commander of Air Force Cyberspace Command argues that a novel aspect of cyberwarfare is its inherently asymmetric nature, saying, 'the price of admission is inexpensive. It's a laptop computer and a connection to the Internet.' Glenn Derene, 'The Coming Cyberwar: Inside the Pentagon's Plan to Fight Back', *Popularmechanics.com*, n.d., <www.popularmechanics.com/technology/military/4277463>. Other experts argue that an inferior adversary could turn 'the United States' sophisticated arsenal of space-age weapons [...] against us to devastating effect'. Clarke and Knake, *Cyber War*, 93.

[16] For example, many Chinese military analysts believe that Operations 'Desert Storm', 'Enduring Freedom', and 'Iraqi Freedom', as well as the US military campaign in the Balkans, revealed logistics and force deployment times to be the potential Achilles' heel of US force projection. Northrop Grumman Corporation, *Capability of the People's*

cyberattack could be launched against US critical *civilian* infrastructure in a manner that completely bypasses military defenses. Widespread vulnerabilities to distributed denial-of-service (DDoS) attacks, network intrusions, viruses and malware suggest that CNA may be particularly useful for fomenting crises, including environmental disasters and large-scale power outages.[17] The US military's growing dependence on commercial off-the-shelf products, many of which are made overseas, and the growing number of operational control systems (e.g., SCADA (Supervisory Control and Data Acquisition systems) and ICS (Industrial Control Systems)) that are connected to an IP (Internet Provider) network have made both military and civilian infrastructure increasingly vulnerable to cyberattack.[18] Supposedly exacerbating US vulnerability is the fact that, unlike most powerful conventional weapons, many of the basic computers and electronic technologies necessary to carry out CNA are increasingly affordable for most states.

A second reason why cyberwarfare may function as a 'great equalizer' is that in cyberspace the geographical distance between the attacker and the target is basically irrelevant. Everything being equal, it is basically as easy to launch a cyberattack against a geographically contiguous system or network as one halfway across the world (or in orbit).[19] A state that has invested in developing a sophisticated cyberwarfare capability may not need to use its limited resources to build a (more) expensive physical weapons platform such as an aircraft carrier in order to 'project force' and coerce a distant adversary.[20] This fact reduces the significance of the 'guns vs. butter' trade-off by lowering the costs of developing a force projection capability. Furthermore, CNA may allow the attacking state to project force without placing conventional forces in harm's way or reducing homeland defenses to deploy units to a distant theater, thereby (potentially) further lowering the expected costs of an attack.

Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Prepared for US–China Economic and Security Review Commission, 16 Oct. 2009, 25.

[17] A recent global survey commissioned by McAfee found that 29 per cent of operators of critical infrastructure reported having suffered large-scale DDoS attacks multiple times each month: 89 per cent had experienced infection with a virus or malware. Stewart Baker *et al.*, *In the Crossfire: Critical Infrastructure in the Age of Cyber War* (Santa Clara, CA: McAfee 2010), 5.

[18] Connections to the Internet or other IP networks may allow unauthorized users access to core systems. Ibid., 19.

[19] What is of relatively greater importance than the target network's physical distance is its level of security and whether it is air-gapped.

[20] It is important to note that some advanced forms of CNA, such as Stuxnet, will require large investments of time and financial resources. For insight into the complexity of Stuxnet, see Falliere *et al.*, *W32.Stuxnet Dossier*.

What are the implications of this alleged leveling of the playing field? If one believes that states only engage in conflicts that they expect to win or from which they expect to at least yield a net gain, one would conclude that proliferation of any technology that lowers the weaker state's estimation of the power/capabilities gap between it and its stronger adversary can be expected to make war more likely.[21] Second, in the same way that the nuclear revolution had a stabilizing effect on the postwar international system by significantly increasing the costs of war, the (real or imagined) expected *reduced* cost of engaging in cyberwar relative to conventional war may make states more likely to invest in developing the necessary capabilities, and if successful, use them.

However, any analysis that stops here is incomplete. At least two countervailing factors should limit the likelihood of a conventionally inferior actor launching a cyberattack against a superior adversary. First, in most cases a rational, relatively weak actor will probably *only* engage in asymmetric warfare when its objectives are limited.[22] Although a basic CNA capability may be *relatively* easy to acquire, effectively prosecuting an attack against moderately defended systems, much less one that would cripple the infrastructure of a sophisticated adversary, would require significant human capital, technical, and organizational capabilities, which in most cases will be out of reach for conventionally weak actors.[23]

Second, most assessments of cyberwarfare's asymmetric utility focus exclusively on how the acquisition of CNA capabilities would affect the weaker actor's strategic calculations; the implicit (and facile) logic underpinning these analyses is basically tantamount to the following: 'if an actor possesses a capability to exploit an adversary's vulnerability, it will use it.' The resulting expectation is that wars will become more frequent as weaker actors perceive shrinking capability gaps between themselves and their stronger adversaries. However, such analyses fail to recognize that war is rarely a one-sided act. Rational actors will not engage in costly wars if they can reach a negotiated bargain by other, less costly, means. This typically holds for both sides in a potential conflict, regardless of their relative strengths. In a coercive context, we should expect the proliferation of cyberwarfare capabilities to provide conventionally weaker powers with a stronger deterrent against

[21] As Blainey writes, 'Recurring optimism is a vital prelude to war. Anything which increases that optimism is a cause of war. Anything which dampens that optimism is a cause of peace.' Geoffrey Blainey, *The Causes of War*, 3rd ed. (New York: Simon and Schuster 1988), 53.

[22] Rattray, *Strategic Warfare in Cyberspace*, 196.

[23] Ibid, 163–234.

their stronger adversaries. In such a scenario, the expected outcome of the strategic interaction would not be war but a negotiated resolution of the dispute in a manner in which the stronger state offers its adversary a better bargain than it would have otherwise. Thus, in some cases the proliferation of cyberwarfare capabilities may actually *decrease* the frequency of war by both making conventionally stronger actors more reluctant to pursue belligerent foreign policies and reducing the credibility of their threats to use force against weaker actors.[24]

CNA and the Difficulty of Attribution: Plausible Deniability

Hypothesis 2: Plausible deniability and the difficulty of attributing cyberattacks may lead actors to become less fearful of retaliation and use CNA against adversaries that they would not dare attack with conventional weapons. Possible misattribution on the part of the recipient of the attack, coupled with the possibility of subsequent escalation, will increase the frequency of war.

Another aspect of cyberwarfare that has become a significant source of concern is *plausible deniability*, which is defined as the ability of actor A (the attacker) to launch a cyberattack against actor B (the target) in a manner such that it is difficult to prove A's responsibility. This unique aspect of cyberattacks may lead some actors to conclude that cyberattacks can be launched with relative impunity, thus lowering the potential aggressor's expected costs and making the use of CNA more likely than conventional force. In this view, there are at least three reasons why plausible deniability may increase the frequency of war.

First, there is nothing approaching a state monopoly on the use of 'force' in cyberspace. Suppose A and B are states. Even if B is able to prove that a cyberattack was launched from computers within A, A may be able to parry the accusation by claiming that the attack was launched by a non-state actor without A's knowledge or sanction. In other words, even if A is directly responsible for the cyberattack or is complicit in an attack launched by a non-state actor within A – e.g., a 'cyber-nationalist' group – it would be very difficult for B to prove that A's government willfully 'pulled the trigger'. Without clear evidence directly linking A to the cyberattack, B may find it difficult to justify a counter-attack (in kind or using kinetic force) to the international

[24] At the same time, war could result if bargaining breaks down as a result of inconsistent beliefs about the two side's relative capabilities. In addition to the weaker power having 'incentives to misrepresent', the nature of cyber 'weapons' (computer code) makes transparency of actual capabilities difficult, if not impossible. In some situations, weaker powers may feel the need to demonstrate their capability in order to obtain a more favorable outcome in the bargain.

community. Thus, the difficulty of identifying the origin of a cyberattack may weaken B's ability to deter A.

Second, the nature of cyberspace is such that attacks could be launched by proxy.[25] For example, even if the source of an attack against B is accurately traced to computers within A, it is possible that the true culprit is state (or terrorist group) C, who launched the attack via computers in A without A's knowledge or sanction. An actor could take advantage of this possibility to engage in strategic 'cyber-framing.'[26] This kind of attack will be expedient if C has a strategic incentive to incite a conflict between A and B. It will be particularly effective if it is launched in the context of a dispute or crisis between the two other actors.[27]

Although not a case of cyber-framing, the events following a series of DDoS attacks on US government websites in July 2009 evince similar dynamics, in particular the possibility that in the context of a crisis a cyberattack could be misattributed and result in a knee-jerk retaliatory strike based on circumstantial evidence. This incident serves as a cautionary tale of how the difficulty of attributing CNA may lead to unnecessary crisis escalation and war.[28]

Third, the ability plausibly to deny a cyberattack may be particularly expedient when an actor believes that a 'brute force' attack can be launched against specific physical infrastructure with impunity (e.g., Stuxnet).[29] If the attacker miscalculates and the target successfully

[25] A simple example is a DDoS attack using a botnet based in a third country.

[26] This concept is roughly analogous to what Libicki terms a 'false flag.' Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation 2009), 89.

[27] Security scholars may note a parallel to concerns about the possibility of nuclear 'catalytic war' during the 1960s and 1970s. The concept may be much more applicable to cyberwar than nuclear war, at least as long as the ability to trace cyberattacks does not improve significantly and proliferate to most states in the near future. Some analysts suggest that a state could even use such a cyberattack to draw an ally into a potential or hot conflict between itself and a third state. Clarke and Knake, *Cyber War*, 213. However, any attempt to do so would require a state to attack an ally; a very risky move. The author is indebted to Aaron Friedberg for suggesting this parallel to 'catalytic war.'

[28] In July 2009, government websites in the US and South Korea were struck by DDoS attacks. In response to these attacks the top-ranking Republican on the House Intelligence Committee demanded a 'show of force or strength' against North Korea. Fortunately, the Obama administration did not heed his calls – a year later US officials largely ruled out North Korea as the source of the attack. Kim Zetter, 'Lawmaker wants 'show of force' against North Korea for website attacks', *Wired.com*, 10 July 2009; Lolita Baldor, 'US largely ruling out N. Korea in 2009 cyberattacks', *Associated Press*, 3 July 2010.

[29] Alternatively, non-attributable operations could be used 'for the purpose of conducting network reconnaissance and implanting the means to execute attacks

identifies the source of the cyberattack via cyber-forensics or because the attack occurred in the context of a bilateral crisis, the risk of subsequent escalation will be relatively high.

The three reasons delineated above suggest that the proliferation of cyberwarfare capabilities may cause a net increase in the frequency of war. Ostensibly, the difficulty of attributing cyberattacks may lead states to initiate or provoke wars that they would otherwise avoid. However, such logic overlooks the fundamental fact that war usually has political objectives. Under most circumstances, *any would-be aggressor who does not identify itself forfeits the ability to coerce its adversary*. An actor must identify itself in order to make a demand and extract a concession; otherwise there is no way for the target to understand what it must do (or not do) in order to forestall or stop the attack. In other words, plausible deniability may be irrelevant when the objective of a cyberattack is coercive. Once one understands that 'cyberwarfare' will usually occur in the context of a political, strategic interaction or bargain between two or more actors, rather than on the unilateral whim of a single actor, its allegedly grave implications for international stability become significantly less disconcerting.

CNA and the Offensive Advantage?

Hypothesis 3: The difficulty of defending against cyberattacks renders states exceedingly vulnerable to surprise attacks. Because states cannot afford to not attack first, the 'offensive advantage' of CNA will increase the frequency of preemptive war.

Brodie called the atomic bomb 'the absolute weapon' because there was no defense against it. A few years earlier, Major General Giulio Douhet and others made similar arguments about airpower.[30] Similar claims have been made about cyberwarfare; a number of analysts have expressed particular concern about its usefulness in a surprise attack.[31] Why? Two aspects of the cyber-domain suggest that for the foreseeable future cyberwarfare may provide a significant offensive advantage.

immediately at the onset of hostilities'. Jan Van Tol *et al.*, *AirSea Battle: A Point-of-Departure Operational Concept* (Center for Strategic and Budgetary Assessments 2010), 56.

[30] Douhet once said, 'Viewed in its true light, aerial warfare admits no defense, only offense'. Quoted in Rattray, 'An Environmental Approach to Understanding Cyberpower', 260; For an overview of air bombardment theory and its flaws, see Rattray, *Strategic Warfare in Cyberspace*, 235–308.

[31] For example: Clarke and Knake, *Cyber War*, 157–8; Andrew Krepinevich, 'The Pentagon's Wasting Assets', *Foreign Affairs* 88/4 (Aug. 2009), 31; Libicki, *Cyberdeterrence and Cyberwar*.

If seminal work in the offense-defense literature is correct, these characteristics suggest that as more and more actors acquire CNA capabilities cyberwarfare's offense-favoring nature could lead to a higher frequency of crisis escalation and war.[32]

First, using existing technologies CND is technically difficult and, relative to the costs of developing a CNA capability, expensive. CNA against civilian infrastructure can completely bypass military defenses. In the US case, even if the technologies necessary to reliably defend civilian networks are feasible it may not be possible for the government or military to secure the thousands of vulnerable existing critical networks.[33] Additionally, many advanced CNA may utilize 'zero-day exploits', that is, attacks aimed to exploit latent vulnerabilities of which the user (and designer) are unaware. In order to recover from such an attack, the exploited vulnerability must be identified and fixed; either step may be very time-consuming. In short, the difficulty of defending against a surprise attack launched against military-affiliated logistical networks or a 'decapitation' attack launched against command and control systems – which could potentially cripple the target state's conventional military forces and dramatically increase the effectiveness of any subsequent use of conventional force – suggests that cyberwarfare capabilities may significantly favor the offensive advantage.[34] In a crisis situation in which defense is difficult or impossible, leaders on both sides may feel pressure to attack before being attacked, lest their non-cyber forces be rendered ineffective by the adversary's first strike.

A second reason why CNA may provide more of an offensive advantage than many conventional weapons is that – if sufficient preparations (e.g., reconnaissance, such as mapping of adversary systems) are made in advance – it often significantly shortens the *time horizon* of an attack. Generally speaking, gains in speed facilitate surprise attacks, which in turn increase both the attacker's security and the defender's insecurity. The same logic applies to cyberwarfare. A

[32] In a seminal article, Van Evera identifies several consequences of an offensive advantage, including: more aggressive foreign policies, an increased risk of preemptive war, more competitive styles of diplomacy, and tighter political and military secrecy. The last consequence may make bargaining failure more likely given its exacerbation of asymmetric information. Stephen Van Evera, 'The Cult of the Offensive and the Origins of the First World War', *International Security* 9/1 (Summer 1984), 58–107; See also Fearon, 'Rationalist Explanations for War', 402–4.

[33] Many of these networks are owned by private corporations that may not want to grant the government or military the level of access necessary effectively to protect them.

[34] This all presumes, of course, that a tactical CNA against an adversary's military networks would be followed immediately by the use of conventional military force, which would minimize the chances of a retaliatory strike.

shortened time horizon may shift the offense-defense balance in the attacker's favor for three reasons: first, the difficulty of situational awareness when CNA runs its course in a few seconds and offers no observable warning signs that an attack is imminent. Second, in the domain of cyberspace, 'geography' favors the attacker by shortening the time it takes for an attack to reach its target given the absence of physical ground and barriers to slow down an attack. And, third, a surprise cyberstrike that disrupts or disables an adversary's military networks could be followed by a conventional attack that permanently destroys or disables the adversary's physical weapons and/or networks before it is able to bring them back online. Such an attack – referred to in this article as a 'cyber-plus' attack – could have a devastating impact on the target state's capacity to retaliate using conventional force – thus shifting the conventional balance in the attacker's favor, at least temporarily – and, in some circumstances (such as when the attacker's objectives are limited), constitute a fait accompli.[35]

Although the difficulty of cyberdefense means that many existing military and civilian networks are susceptible to cyberattack, circumstances may not be as dire as is often assumed. First, in most cases, a cyberwarfare capability is unlikely to change the conventional balance sufficiently to render CNA expedient as a stand-alone tool of coercion. Used in isolation, the disruption and/or damage caused by a successful first cyberstrike will probably be more ephemeral than a kinetic attack; defenders may be able to find and fix vulnerabilities at relatively low cost or quickly reroute data flow to an uncompromised network. In most coercive contexts, CNA will thus be ineffectual as the primary weapon in an extended coercive campaign.[36] It is dubious whether an otherwise weak actor could force major concessions from a conventionally powerful adversary merely by acquiring a cyberwarfare capability.

Rather, CNA would probably be most effective as an opening salvo to disable defenses in immediate advance of a major conventional/nuclear attack aimed at significantly (and permanently) reducing the adversary's ability to retaliate. In other words, CNA will probably be most useful in a coercive context in which the *relatively* weak actor already possesses formidable – even if not superior – conventional capabilities.[37] If a rational actor believes that an offensive advantage

[35] As one cyberwarfare expert notes, 'it is more difficult to measure the intent of an electron than it is to measure the intent of a tank.' Timothy Thomas, Testimony Before the US-China Commission (Transcript), 2001, <www.uscc.gov/textonly/transcriptstx/testho.htm.>

[36] Libicki, *Cyberdeterrence and Cyberwar*, xv.

[37] For example, in the context of a dispute between a superpower and near-peer competitor.

exists and that a first cyberstrike will tilt the conventional balance and significantly increase the likelihood of victory in the subsequent conventional conflict, it may be less willing to moderate its demands when bargaining. Although under circumstances of complete information the weaker side's ability to launch a surprise cyberstrike and shift the conventional balance of power would lead to a negotiated settlement (albeit with improved terms for the weaker side), asymmetric information – specifically, the difficulty of issuing a credible threat to launch a cyber-strike – and a perceived offensive advantage may force a conventionally weaker state to initiate hostilities in order to signal both its possession of cyberwarfare capabilities and willingness to use them, thereby improving its bargaining position.

In sum, although CNA may be expedient as a brute force weapon/force multiplier, the expected net effect of its offensive advantage on the frequency of war will be marginal. CNA capabilities will probably only increase the likelihood of war in a coercive diplomacy situation when there is a relatively small gap in the conventional balance of power between two actors *and* inconsistent beliefs about each other's actual capabilities. The idea that a weak actor could coerce a superpower merely by threatening or launching a cyberattack without a formidable conventional or nuclear capability to follow through rests on dubious grounds.

CNA and Cyberdeterrence

Hypothesis 4: The challenges inherent in attributing CNA, developing active cyberdefenses (and thus the ability to credibly threaten retaliation), and instituting robust arms control agreements in order to prevent destabilizing spirals will make it difficult to deter potential aggressors and thus increase the frequency of war.

This section first examines the practicality of deterrence in a hypothetical world in which escalation outside of the cyber-domain is impossible.[38] Next, it examines the more realistic scenario of deterrence in the context of a political bargain in which both actors are identified and escalation to a higher level of conflict is possible.

The difficulty of cyberdeterrence ostensibly has significant implications for the frequency of war in a world in which cyberwarfare capabilities have proliferated, as states without a strong deterrent may find it more difficult to disincentivize the coercive use of CNA against them. Effective deterrence requires the would-be target to signal to a potential aggressor that it possesses at least one of two capabilities:

[38] Some analysts call this 'deterrence in kind'. Libicki, *Cyberdeterrence and Cyberwar*, 27.

the ability to field an effective defense and/or the ability credibly to threaten the would-be attacker's interests. The first, sometimes called 'deterrence by denial', is aimed at reducing the attacker's expectation that an attack will succeed. The other, 'deterrence by punishment', is aimed at influencing the attacker's intentions through both a credible threat to retaliate against its core interests in the event of an attack and reassurance that the actor will withhold punishment if not attacked.[39]

Let us first examine a hypothetical scenario in which conflict is restricted to the cyber-domain. Because offense dominates in the cyber-domain and the cost of developing a CNA capability is *relatively* low, deterrence by denial is difficult. However, the implications of the difficulty of passive CND for deterrence are not as dire as much of the public debate would suggest. Why? Many observers base their pessimistic conclusions about the difficulty of cyber deterrence on a misconception that passive CND is *necessary* for effective deterrence.[40] Such an argument conflates defense and deterrence.

The objective of defense is to reduce one's own costs in the event that deterrence fails.[41] Far from being necessary, the unilateral expansion of defensive capabilities will often not lead to greater stability between states.[42] Nuclear deterrence suggests that a strong defense may not even be necessary to deter a would-be adversary. In contrast, a credible capability to retaliate (i.e., deterrence *by punishment*) is much more likely to do so. There are two conditions that together are sufficient for effective deterrence: the ability credibly to threaten the other state's core interests in the event that it attempts to overturn the status quo, and assurances that compliance will not result in major punishment.[43]

Unfortunately, without a credible threat to retaliate, such as an active defense capable of promptly identifying the source of the attack and quickly launching a counterattack, even this kind of cyberdeterrence may not be feasible when escalation outside the cyber-domain is not

[39] Deterrence targets the enemy's intentions, while defense aims at reducing his capabilities. Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton UP 1961).

[40] For examples of such claims, see Clarke and Knake, *Cyber War*, 157; Richard Hayes and Gary Wheatley, *Information Warfare and Deterrence*, NDU Press Book (Washington DC: National Defense University 1996), 11.

[41] From this point on, 'defense' refers specifically to passive defense unless otherwise noted. The aim of passive defenses is to minimize the damage caused by hostile attack without taking the initiative. Examples include fortifications and moats. Active defense refers to area denial, i.e., the use of limited offensive force and counterattacks.

[42] Robert Jervis, 'Cooperation Under the Security Dilemma', *World Politics* 30/2 (Jan. 1978), 167–214.

[43] Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale UP 2008).

possible. Even if the target eventually succeeds in accurately identifying the source of the attack, the tracing process itself would be time-consuming; this response lag time significantly reduces the credibility of any threat to launch a cyber counter-attack. Although, as discussed above, the attribution problem is not a major concern in a coercive context, deterring CNA strictly in the cyber-domain may be impossible when the attacker does not need to identify itself (e.g., when the objective is anonymous destruction).[44]

Let us next assess the difficulty of deterrence in a more realistic scenario in which escalation to a higher level of conflict is possible and the objective of cyberwarfare is political (coercive). A common misconception about cyberdeterrence is that a public, explicit, and blanket declaration to the effect that all attacks against the state – cyber or otherwise – will invite a conventional or nuclear response is sufficient to establish a credible deterrent against cyberattacks.[45] US champions of such arguments frequently call on Washington to publicly issue an unequivocal warning that the US military will respond to any attack against US military or civilian interests – be it a conventional, nuclear, or cyberattack – with military force.[46] There are several reasons why such deterrence efforts will probably be ineffective.

First is the stability-instability paradox, which suggests that while nuclear- or conventional-based deterrence may be sufficient to sharply reduce the probability of a direct nuclear or conventional exchange between two or more actors, it may simultaneously increase the probability of a minor conflict between them at a lower level of conflict; in this case, in the cyber-domain. Seeking to avoid potentially catastrophic nuclear or conventional war and assuming that neither side will allow a cyber exchange to escalate, a potential aggressor may be more willing to use CNA in order to coerce its adversary, particularly when its strategic objectives are limited.[47]

[44] For more on the limited relevance of the attribution problem to cyber deterrence, see Richard Kugler, 'Deterrence of Cyber Attacks', in Kramer *et al.*, *Cyberpower and National Security*, 317–20.

[45] For example, some experts call for ensuring cyberdeterrence by developing a 'cyber countervailing' strategy analogous to the countervailing nuclear strategy adopted by NATO during the Cold War, which '[made] known to the adversary that the implication of a nuclear strike would be far greater than the potential gains an adversary could achieve by initiating the first strike'. Amit Sharma, 'Cyber Wars: A Paradigm Shift from Means to Ends', *Strategic Analysis* 34/1 (2010), 69.

[46] Similarly, a recently proposed law in Russia aims to give Moscow the authority to treat a cyberattack of any kind as an act of war and respond accordingly. Baker *et al.*, *In the Crossfire*, 30.

[47] For example, Chinese military doctrine appears to be consistent with this view. China's 'Science of Military Strategy' notes that many PLA Information Warfare

Second, deterrence may only work to the extent that the would be-target has a credible threat to retaliate appropriately and proportionately to an attack at any level of conflict. Bold policy declarations are insufficient; a credible deterrent threat requires either that the state possesses a known capability to defeat adversaries at every possible level of conflict, or escalation dominance with a credible means *and the will* to escalate the conflict to a higher level (e.g., to retaliate to a cyberattack with conventional military force). For example, the US certainly has the capability to escalate a cyberwar to a higher level of conflict in which it enjoys dominance; what is uncertain is whether or not it has the will. The US conventional and nuclear deterrents may be relatively ineffective against a 'cyber-armed' adversary if the adversary believes that the US will not react to a cyberattack with a cross-domain response.[48] Last, a blanket policy declaration that states that *all* attacks will be met with a forceful military response could quickly lose credibility unless the state in question defines a clear threshold as to what kind of CNA will invite an escalatory response.

A third issue that complicates cyberdeterrence is the impracticality of forestalling destabilizing spirals through arms control and mutual efforts to improve transparency.[49] First, the relevant platforms (computers) and weapons (computer code) are essentially uncountable.[50] Second, stable deterrence depends heavily on information about the weapons themselves *and* the associated military doctrine and command and control.[51] To date, no state has been forthcoming with such information. Asymmetric information due to low levels of transparency, coupled with clear incentives to misrepresent actual capabilities, may lead to disparate perceptions about each side's relative strength, miscalculation, and war.

A fourth issue that further complicates cyberdeterrence is the fact that most cyberattacks will probably have minimal human casualties. The ambiguity surrounding the applicability of existing international

operators believe CNA to be 'bloodless;' thus CNA 'may become first choice weapons for a limited strike against adversary targets to deter further escalation of a crisis'. Northrop Grumman Corporation, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, 19.

[48] James Lewis, 'Cross-Domain Deterrence and Credible Threats' (CSIS, July 2010).

[49] Despite this, the US and Russia recently began talks with a UN arms control committee about limiting the military use of cyberspace. 'In shift, US talks to Russia on internet security' *New York Times*, 13 Dec. 2009. Most analysts are cynical about its prospects.

[50] Unlike other arms control efforts that destroy weapons, cyber arms control can only forbid certain acts; it cannot eliminate capability. Clarke and Knake, *Cyber War*, 254.

[51] Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell UP 1990), 60.

laws governing the use of force to hostile acts in cyberspace, coupled with the principle of proportionality, may lead less reputation-conscious actors to judge that cyberattacks can be launched against reputation-conscious states with relative impunity. The attacker may assume that even if the attack is attributable the target would be unwilling to either escalate to a higher level of conflict or, if the attack was launched against civilian infrastructure, retaliate in kind. In short, the potential aggressor may calculate that the expected benefits of an attack outweigh the (relatively low) expected costs. As a result, it may be more inclined to drive a hard bargain. Again, disparate perceptions may lead to a breakdown in negotiations and war.

Despite the afore-mentioned difficulties inherent in deterring cyberattacks, there are at least two mitigating factors that should reduce the likelihood that CNA will be used, at least in circumstances where the attacker's objective is coercive. First, the *relatively* high level of uncertainty about the consequences of CNA, coupled with the possibility of self-inflicted damage, may have a countervailing effect on the incentive to take risks and thereby lower the expected utility of an attack. In contrast to most modern kinetic weapons, it is difficult to predict both the probability of success of CNA and its second- and third-order effects.[52] An attack against any target system on a non-air-gapped network could have unintended ramifications that may harm the attacker's own interests.[53] This risk may take otherwise strategically desirable targets (e.g., the US banking system) off the table. Furthermore, the intense secrecy surrounding states' cyberwarfare capabilities means that an attacker may not be completely certain whether the target actor possesses effective active defenses that could be used to launch a retaliatory strike. In short, the relatively high uncertainty of the possible ramifications of a cyberattack may itself function as a kind of deterrent against the use of CNA.

The second reason that the difficulty of cyberdeterrence may not result in a significant increase in the frequency of war is that warfare usually occurs within the context of a strategic bargain between two or more clearly identifiable actors. Whether deterrence is effective or not will be determined by both a given actor's cyberwarfare capabilities and its ability to retaliate at higher levels of conflict. Although, as discussed above, this fact may not allow the actor to deter *all*

[52] Vice Admiral Bernard McCullough, 'Positioning the Navy for Cyber Warfare: US Fleet Cyber Command' (Center for Strategic and International Studies, 5 April 2010), <http://csis.org/event/cyber-warfare>.

[53] Lewis, 'Cross-Domain Deterrence.' For example, more than 40 per cent of the systems infected by the 'precision' Stuxnet malware were in 154 countries *aside from Iran*. Falliere *et al.*, *W32.Stuxnet Dossier*, 6.

cyberattacks with certainty (especially against less reputation-conscious adversaries), it is likely that it will be able to deter most severe cyberattacks.[54]

Part 2: Implications for Bargaining Dynamics and the Probability of War in Four Scenarios

The analysis in Part 1 suggests that the net effect of the proliferation of cyberwarfare capabilities on the probability of war between actors in the international system will not be constant across all situations. This section explores the manner in which cyberwarfare capabilities may affect perceptions, bargaining dynamics, and the probability of war between actors in four ideal-type dyads. The analysis, which is informed by a rationalist bargaining theory of war, suggests that although in some situations the proliferation of cyberwarfare capabilities may affect one or both sides' actual *and perceived* bargaining strengths in such a way that war becomes more likely because of the two sides' inability to reach a mutually acceptable settlement, in other situations it may have a powerful deterrent effect, thus decreasing the probability of war. Consistent with the analysis in Part 1, a constant across all scenarios is CNA's utility as a brute force tool.

Terrorist Group vs. State

Concerns about the possibility of cyberterrorism against the US have increased since September 11, 2001.[55] At first glance, CNA seems to be the ideal weapon for a terrorist group. Not only are the weapons thought to be inexpensive and relatively easy to acquire, physical distance is irrelevant and much of the developed world's critical civilian infrastructure is relatively vulnerable. The attribution problem would seem to make CNA particularly attractive to terrorists, who are often not only risk-acceptant but also may not have a 'mailing address' or infrastructure against which their target could eventually launch a retaliatory strike. Furthermore, the immediate objective of most terrorist attacks is often destruction (brute force) or to provoke a conflict between two other actors via cyber-framing. If Rattray is correct to suggest that 'waging strategic information warfare might prove most useful [...] for actors whose political objectives are limited in scope, who can control vulnerability to retaliation, and who possess a willingness to take risks', then terrorists seem to be probable users.[56]

[54] The argument here differs from that of analysts who argue that deterrent theory does not apply to cyber warfare. E.g., Clarke and Knake, *Cyber War*, 189–95.

[55] Kugler, 'Deterrence of Cyber Attacks', 317.

[56] Rattray, *Strategic Warfare in Cyberspace*, 101.

Despite the ostensible appeal of 'cyberterrorism' to terrorist groups, over the past decade no incident of terrorism has involved a cyberattack. Why? First, one reality that is often overlooked in analyses that focus primarily on states' vulnerabilities to cyberattacks is the difficulty of developing the technical and organizational capacity necessary to launch sustained, simultaneous cyberattacks against multiple targets. Possession of such capabilities is a prerequisite for any terrorist group aiming to cause sufficient disruption to threaten seriously the interests of a state and/or coerce its leaders.[57] Second, even if a terrorist group is able to launch such complex attacks, it is doubtful that they would generate the level of widespread panic and terror which terrorists desire.[58] In short, although widespread vulnerabilities in critical infrastructure seem to present easy targets for terrorist groups, the consequences of an attack are probably insufficiently disastrous to warrant the opportunity cost in time and money necessary to *attempt to* develop the necessary organizational and technical capacity.

Although the kind of cyber attacks necessary to seriously threaten states' interests and coerce their leaders are probably beyond the reach of most terrorist groups, isolated brute force attacks against small numbers of targets may be feasible. Their effects, however, are more likely to annoy the target state than anything else.

Strong State vs. Superpower

Generally speaking, from the perspective of a conventionally preponderant superpower, the marginal strategic utility of a CNA capability is limited. It will, however, be useful as a difficult-to-attribute brute force measure against an adversary's military or civilian infrastructure (e.g., Stuxnet).

Of greater significance is the effect that the advent of cyberwarfare may have on a superpower's perceived vulnerability to attack. For example, if a superpower's leaders judge that the computer networks upon which their military relies to project conventional force are vulnerable, they may be less inclined to escalate bilateral political conflicts or intervene in disputes between other actors when they believe the adversary possesses a 'cyber-plus' attack capability.[59] In short, in this scenario the net effect of the advent of cyberwarfare is to

[57] Irving Lachow, 'Cyber Terrorism: Menace or Myth', in Kramer *et al.*, *Cyberpower and National Security*, 442–7.

[58] Critical infrastructure already fails fairly regularly (e.g., blackouts) – often for banal reasons such as human error – without generating widespread panic. Ibid., 447–8.

[59] I.e., both robust CNA and conventional capabilities.

lower the probability that, other things being equal, a superpower will initiate a war against a strong state.

From the perspective of the strong state, the ability to launch CNA may represent a valuable counter-force and counter-value weapon by which to threaten the superpower's forward-deployed and superior conventional forces and its geographically-distant civilian infrastructure, respectively.[60] This may tilt the power balance between the two states sufficiently to deter the superpower from escalating or intervening in a conflict between the strong state and a third party, thus reducing the probability of war between the two states.[61]

However, there are at least two scenarios in which disparate perceptions – *asymmetric information* – about relative power and resolve may render a mutually-acceptable bargain unattainable, thereby increasing the probability of war between the superpower and the strong state. The first scenario is one in which the strong power believes that the superpower is more vulnerable to a cyberattack against its conventional military forces than the superpower believes itself to be. This may be a consequence of the strong state's inability to convince the superpower *ex ante* that it in fact possesses an effective cyberattack capability. The second scenario is one in which the strong state's objectives are limited and it underestimates the superpower's resolve and willingness to escalate to a higher level of conflict. In other words, in this scenario disparate perceptions about relative resolve may weaken the superpower's conventional deterrent.

Weak State vs. Strong State/Superpower

The dynamic at play in this scenario is analogous to that involved in the previous scenario with one key exception: both sides understand that the weak state lacks the capability to follow through on a surprise cyber counter-force attack with a conventional strike; thus, disparate perceptions about each side's relative strength are unlikely to lead to war. On the other hand, the weaker state's ability to launch counter-value cyberattacks against a conventionally superior and network-dependent adversary's civilian infrastructure means it is in position to inflict unacceptable costs. It is in this situation that the truly 'asymmetric' potential of CNA is most relevant; CNA may give weaker states leverage over conventionally superior adversaries that they would

[60] In the scenario envisioned here, without CNA the superpower's civilian infrastructure would otherwise be out of range of the strong state's conventional weapons.

[61] For example, Chinese doctrinal writings on information and cyberwarfare suggest that the scenarios described here may be applicable to a potential conflict between the US and China over Taiwan.

otherwise not enjoy. However, because of the weaker state's inability to follow through on a cyberattack with conventional force, in most of these situations CNA's strategic utility will be limited to deterring its stronger adversary from coercion or escalating a crisis.

Despite the relatively low cost of developing a cyberwarfare capability it is doubtful that states at the lower end of the weak state spectrum will be able to develop the organizational and technical capacity necessary to launch sustainable cyberattacks against multiple (and perhaps partially-defended) targets in a stronger state. Additionally, to the extent that the weak state is able to develop CNA capabilities, the involved systems will probably be heavily reliant on non-proprietary technologies and thus highly vulnerable to retaliation.

Last, it should be noted that from the perspective of the more powerful state the ability to use CNA as a coercive or brute force tool may be irrelevant if the target state's infrastructure is so underdeveloped that high-value targets are not network-dependent.[62]

Weak State vs. Weak State

The fact that both sides in this scenario may have severely limited abilities to project conventional force may mean that a cyberwarfare capability provides these states with a new, relatively affordable weapon with which to coerce an adversary. Limited conventional capabilities on both sides mean that the risk of escalation is low; as a result, a protracted 'cyberwar in-kind' may be possible.

Summary of Preliminary Analysis from Part 2

The above analysis suggests that fears of CNA as a destabilizing weapon, although warranted, may be exaggerated. CNA's usefulness to a relatively weak state or terrorist group as an asymmetric weapon is restricted to a small number of situations. In some situations it may actually *decrease* the frequency of war by offering relatively weak states a useful deterrent against belligerent adversaries. Plausible deniability only seems to be expedient in brute force attacks (possible in all scenarios) and, at least theoretically, as a strategic weapon in instances of cyber-framing. The difficulty of CND both contributes to the usefulness of CNA as an asymmetric weapon and suggests that brute force attacks by sophisticated states against specific infrastructure will become increasingly frequent. However, this will only remain the case

[62] Libicki, *Cyberdeterrence and Cyberwar*, 70. In contrast, all states – regardless of development phase – have physical structures that can be threatened by kinetic weapons.

if the technical obstacles to effective CND prove insurmountable – or prohibitively expensive – for most states. Finally, when war is viewed as the outcome of a bargaining process between identifiable actors rather than as a unilateral act which occurs *ex machina;* many of the arguments about the difficulty of deterrence in kind become significantly less disconcerting.

Conclusion

Is cyberwarfare a new 'absolute weapon?' Probably not. Those who claim otherwise may fall into a similar trap to that of early airpower theorists, who 'created a paradigm of strategic warfare with few political constraints [and] neglected the fundamental question of how strategic bombardment translated into political influence'.[63]

Although the proliferation of cyberwarfare capabilities may have the net effect of increasing the frequency of war, much of the public debate on cyberwarfare is excessively pessimistic. Cyberwarfare appears to be a tool for states to pursue political (strategic) and/or military (tactical) objectives at relatively low cost only under very limited circumstances. Although Stuxnet manifests cyberwarfare's potential to become a useful *brute force* measure, no examples of irrefutably effective *coercive* CNA exist. Cyberattacks against Estonia in 2007 were an example of 'hacktivism', not war.[64] Although the 2008 cyber exchange between Georgia and Russia better fits the bill, the attacks had no measurable impact on bargaining or the war's outcome. Thus, CNA's most 'game-changing' aspect may be its usefulness as a brute force weapon, which will probably have at most a marginal effect on the frequency of war. In short, although gradual proliferation of cyberwarfare capabilities may be inevitable, the widespread *use* of CNA is probably not.

Acknowledgments

For valuable comments on earlier drafts of this article, I wish to thank Aaron Friedberg, Jon Lindsay, Jacob Shapiro, participants in the Princeton International Relations Seminar, and an anonymous reviewer.

[63] Rattray, *Strategic Warfare in Cyberspace*, 83–4.

[64] Irving Lachow, 'Cyber Terrorism: Menace or Myth', in Kramer *et al*., *Cyberpower and National Security*, 441.

Note on the Contributor

Adam P. Liff is a Doctoral Candidate in the Department of Politics at Princeton University. He is also a Minerva Scholar, a SPF Non-Resident Fellow at Pacific Forum CSIS and the Sasakawa Peace Foundation, and a Bradley Fellow.

Bibliography

Baker, Stewart, Shaun Waterman, and George Ivanov, *In the Crossfire: Critical Infrastructure in the Age of Cyber War* (Santa Clara, CA: McAfee 2010).

Baldor, Lolita. 'US largely ruling out N. Korea in 2009 cyberattacks', *Associated Press*, 3 July 2010.

Blainey, Geoffrey, *The Causes of War,* 3rd ed. (New York: Simon and Schuster 1988).

Broad, William J. *et al.*, 'Stuxnet worm used against Iran was tested in Israel', *New York Times*, 15 Jan. 2011.

Brodie, Bernard. *The Absolute Weapon: Atomic Power and World Order* (New York: Ayer 1946).

Clarke, Richard, and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco 2010).

Clausewitz, Carl von, *On War* (Harmondsworth, UK: Penguin 1982).

Courville, Lt. Col. Shane P., *Air Force and the Cyberspace Mission: Defending the Air Force's Computer Network in the Future*. Occasional Paper, Maxwell Air Force Base, Alabama: Air War College, Center for Strategy and Technology, December 2007.

Derene, Glenn, 'The Coming Cyberwar: Inside the Pentagon's Plan to Fight Back', *Popularmechanics.com*, nd, <www.popularmechanics.com/technology/military/4277463>.

Falliere, Nicolas *et al.*, *W32.Stuxnet Dossier* (CA: Symantec Security Response 2011), <www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.

Fearon, James D., 'Rationalist Explanations for War', *International Organization* 49/3 (Summer 1995), 379–414.

Fulghum, David A., *et al.*, 'Israel shows electronic prowess', *Aviation Week & Space Technology*, 25 Nov. 2007.

Hayes, Richard, and Gary Wheatley, *Information Warfare and Deterrence*. NDU Press Book. (Washington DC: National Defense University 1996).

Jervis, Robert, 'Cooperation Under the Security Dilemma', *World Politics* 30/2 (Jan. 1978), 167–214.

Jervis, Robert, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell UP 1990).

JP 1-02, DOD Dictionary of Military and Associated Terms, US Department of Defense, April 2010, <www.dtic.mil/doctrine/dod_dictionary/>.

Kramer, Franklin, Stuart Starr and Larry Wentz (eds), *Cyberpower and National Security* (Dulles, VA: Potomac Books 2009).

Krepinevich, Andrew, 'The Pentagon's Wasting Assets', *Foreign Affairs* 88/4 (Aug. 2009), 18–33.

Kugler, Richard, 'Deterrence of Cyber Attacks', in Franklin Kramer, Stuart Starr and Larry Wentz (eds), *Cyberpower and National Security* (Dulles, VA: Potomac Books 2009), 317–20.

Lachow, Irving, 'Cyber Terrorism: Menace or Myth', in Franklin Kramer, Stuart Starr and Larry Wentz (eds), *Cyberpower and National Security* (Dulles, VA: Potomac Books 2009), 441–8.

Lewis, James, 'A Note on the Laws of War in Cyberspace', CSIS, 25 April 2010, <http://csis.org/publication/note-laws-war-cyberspace>.

Lewis, James, 'Cross-Domain Deterrence and Credible Threats', CSIS, July 2010.

Libicki, Martin, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation 2009).

Lord, Kristin M., and Travis Sharp (eds) *America's Cyber Future: Security and Prosperity in the Information Age* (CNAS 2011), <www.cnas.org/node/6405>.

McCullough, Vice Admiral Bernard, 'Positioning the Navy for Cyber Warfare: US Fleet Cyber Command', Center for Strategic and International Studies, 5 April 2010, <http://csis.org/event/cyber-warfare>.

Northrop Grumman Corporation, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. Prepared for US–China Economic and Security Review Commission, 16 Oct. 2009.

Rattray, Gregory, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press 2001).

Rid, Thomas, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35/1 (Feb. 2012), 5–32, <www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939>

Schelling, Thomas, *Arms and Influence* (New Haven, CT: Yale UP 1966).

Sharma, Amit, 'Cyber Wars: A Paradigm Shift from Means to Ends', *Strategic Analysis* 34/1 (2010), 62.

Snyder, Glenn, *Deterrence and Defense: Toward a Theory of National Security* (Princeton UP 1961).

The White House, 'Remarks by the President on Securing Our Nation's Cyber Infrastructure', 29 May 2009, <www.whitehouse.gov/the_press_office/Remarks-by-the-President-on- Securing-Our-Nations-Cyber-Infrastructure/>.

Thomas, Timothy, Testimony Before the US–China Commission (Transcript), 2001, <www.uscc.gov/textonly/transcriptstx/testho.htm>.

US Department of Defense, *Quadrennial Defense Review (QDR) Report*, Feb. 2010.

Van Evera, Stephen, 'The Cult of the Offensive and the Origins of the First World War', *International Security* 9/1 (Summer 1984), 58–107.

Van Tol, Jan *et al.*, *AirSea Battle: A Point-of-Departure Operational Concept* (Center for Strategic and Budgetary Assessments 2010).

Zetter, Kim, 'Lawmaker wants 'show of force' against North Korea for website attacks', *Wired.com*, 10 July 2009.