The Myth of Cyberwar

Bringing War on the Internet Back Down to Earth*

Erik Gartzke†

7 December 2012

Abstract

Cyberwar has been described as a revolution in military affairs, a transformation of technology and doctrine capable potentially of even overturning the prevailing world order. Yet, such conceptions of change reflect a common tendency to conflate means and ends; studying what could happen in cyberspace (or anywhere else) makes little sense without considering how internet conflict is going to accomplish the tasks commonly addressed by terrestrial warfare. To supplant existing modes of conflict, cyberwar must be capable of realizing the political objectives to which force or threats of force are commonly applied, something that in important respects cyberwar fails to do. Cyberwar is much more likely to serve as an adjunct to, rather than a substitute for, existing forms of political violence. Indeed, rather than threatening existing hierarchies, cyberwar appears much more likely to augment the military advantages of status quo powers.

*I thank Eugene Gholz, Jeffrey Kwong and Jon Lindsay for comments and suggestions. Oliver Davies provided research assistance. Please consult with the author before citing.

†University of California, San Diego. E-mail: egartzke@ucsd.edu. Web: http://dss.ucsd.edu/ egartzke.

The next Pearl Harbor we confront could very well be a cyber attack – Leon Panetta

We may be defeated in the first nanosecond of the next war – Daniel T. Kuehl

War is not an exercise of the will directed at inanimate matter – Clausewitz

1 Introduction

A blitz of media, punditry and public pronouncements inform interested observers and policy makers that the next war is likely to be won or lost on the internet. Indeed, events such as the coordinated cyber attacks on Estonia and the Stuxnet worm seem to indicate that cyberwar has already begun. The sense of urgency surrounding cyberwar appears to be tied to perceptions that internet conflict is the newest phase in the ongoing revolution in military affairs, only this time the threat is directed at the sophisticated technological civilizations of the West, rather than at poor developing states or the recipients of inferior second-world military hardware.[1] To believe a growing number of pundits and practitioners, cyberwar threatens to render existing military advantages impotent, exposing those nations most dependent on comprehensive information infrastructures to devastating and unpredictable attacks. If powerful states largely immune to terrestrial invasion can have their military might blunted and their factories and cities idled by foreign hackers, then perhaps this latest technological revolution really does presage a "Pearl Harbor" in which the United States and other great powers will be targets, rather than perpetrators, of shock and awe.

There is a problem with the growing consensus of impending cyber apocalypse, however: it is far from clear that conflict over the internet can actually function as war. Discussions of cyberwar commit a common fallacy of arguing from opportunity to outcome, rather than considering whether something that could happen is at all likely, given the motives of those who are able to act. Cyber pessimism rests heavily on capabilities (means), with little thought to a companion logic of consequences (ends). Much that could happen in the world fails to occur, largely because those capable of initiating action discern no benefit from doing so. Put another way, advocates have yet to work out how cyberwar actually accomplishes the objectives that typically sponsor terrestrial military violence. Absent a logic of consequences, it is difficult to believe that cyberwar will prove

[1] On the revolution in military affairs (RMA), see Toffler and Toffler 1993; Krepinevich 1994, 2002[1992]; Cohen 1996; Hundley 1999; O'Hanlon 2000 and Vickers and Martinage 2004. For criticism, see (Biddle 1998).

as devastating for world affairs and for developed nations in particular as many seem to believe.

This essay assesses the salience of the internet for carrying out functions commonly identified with terrestrial political violence. War is fundamentally a political process, as Clausewitz (1976[1832]) famously explained. States, groups and individuals threaten harm to deter or compel, generating influence through the prospect of damage or loss. Military violence can also be exercised to alter or maintain the balance of power and to resist or impose disputed outcomes. The internet is generally an inferior substitute to terrestrial force in performing the functions of coercion or conquest. Cyber "war" is not likely to serve as the final arbiter of competition in an anarchical world and so should not be considered in isolation from more traditional forms of political violence.[2] In fact, the capacity for internet coercion is limited by the same factors that make cyberwar appear at first to be so intimidating. For threats or demands to prove effective, targets must believe both that an attack is likely to follow from noncompliance, and that the attack is destined to inflict unacceptable harm. Yet, as I detail here, the need to apprise targets of internet vulnerabilities in order to make cyber threats credible contrasts with the secrecy needed to ensure an effective attack.

Since it is difficult to share operational details of planned attacks without compromising military effectiveness, cyberwar must be practiced more often than threatened. Here too, however, there are critical limitations to what can be achieved via the internet. It is one thing for an opponent to idle a country's infrastructure, communications or military capabilities. It is quite another to ensure that the damage inflicted translates into a lasting shift in the balance of national capabilities or resolve. Cyber attacks are unlikely to prove particularly potent in grand strategic terms unless they are accompanied by terrestrial military force or other actions designed to capitalize on temporary weakness effected over the internet. Perpetrators must therefore be prepared to exploit windows of opportunity generated by internet attacks through other modes of combat. Otherwise, there are few compelling reasons to initiate cyberwar in the first place. The chief beneficiaries of cyberwar are thus less likely to be weak or rising powers than those states that already possess important terrestrial military advantages. Conceived of in this way, the internet is less a revolution in military affairs than it is yet another set of technologies that extend existing disparities in power and influence.

[2] "The chief reason warfare is still with us is ... that no substitute for this final arbiter in international affairs has yet appeared on the political scene" (Arendt 1970, page 2).

2 Panic Over the Internet: The Literature on Cyberwar

The nature of war has evolved, if not regularly, then certainly frequently throughout the centuries. As such, it is reasonable, even forward looking, for observers to consider what impact each new technology might have on the nature of war and peace. Innovations like the stirrup, steam propulsion, air transport, and nuclear fission all transformed warfare. Other changes, such as the telephone, high-rise construction techniques and even the advent of effective birth control, may have had less revolutionary than evolutionary effects on political violence. The number and diversity of publications seeking to alert (even alarm) readers about cyberwar is astounding. Yet, for the most part, these studies shine less light on how cyberspace changes the nature of conflict than on what harm could be done over the internet. Below, I review a sample of this work. As can be seen, most studies of cyberwar begin with the conviction that the internet is transforming modern military strategy — detailing either the damage that can be inflicted or problems in countering cyber attack — without showing why harm or an inability to deter necessarily imply a potent military weapon.

2.1 Scope and Scale Conditions of Cyberwar – Cyberpessimists

For many thoughtful commentators, the size of the cyberwar threat could well be unprecedented. Lynn III (2010) argues that cyber-warfare is indeed an imminent threat. Those with a motive to launch an attack against the United States will soon possess the capability to do so. In this sense, cyber-warfare is unique in that those who utilize the strategy are not limited by financial or physical restraints. A vigorous defense as the most viable and flexible strategy in cyberspace. The United States can avoid large-scale cyber calamities through collaboration of public, private, and government-sponsored corporations. Lynn provides Five Pillars of Cyber Space Defense Strategy:

> "treating cyberspace as an operational domain, like land, air, sea, and outer space; employing active defenses to stop malicious code before it affects our networks; protecting commercial networks that operate the critical infrastructure that our military relies upon; joining with allies to mount a collective cyber defense; and mobilizing industry to redesign network technology with security in mind" (Lynn 2011).

Treating cyberspace as an operation domain is an excellent idea, though doing so quickly reveals differences between cyberwar and conflict on land, sea, in the air or in space. It may prove difficult to deter or even defend against cyber attack, but it will prove harder still for an attacker to figure out how to benefit from internet aggression, unless in conjunction with attacks on other domains.

Adams (2001) joins Lynn in arguing that the United States needs a comprehensive cyber-warfare defense strategy. The United States is vulnerable to attack as many smaller nations and private groups will seek to gain an advantage by employing asymmetrical warfare; whose impact would be felt not only in the public sector, but also in private industry (Adams 2001, page 99). Herein lies an interesting paradox, as Adams argues that as the United States increases its military might, it renders itself more vulnerable and prone to ever-increasing incidences of potentially crippling cyber attacks. Shane P. Courville (2007) also considers the United States to be highly susceptible to a catastrophic cyber attack, but he is less optimistic about the ability of the U.S. and other nations to defend themselves. Cyber defense is problematic given rapidly changing technology, and especially given the insecure production of computer hardware. Courville is especially concerned that little thought has gone into exactly who manufactures computer hardware for the U.S. military.

Knapp and Boulton (2006) note that the lack of entry barriers to conducting cyber warfare leave even great powers defenseless against a constant stream of virtual attacks. "Over the past 20 years, wide ranges of formidable cyber-weapons have become more affordable and available, from keystroke and eavesdropping devices to high-energy radio frequency (HERF) and electromagnetic pulse (EMP) generators. An attacker can build an E-bomb, designed to fry computer electronics with electromagnetic energy, for as little as $400" (Knapp & Boulton 2006, page 79). Knapp and Boulton are also concerned that as cyberwar technology advances, U.S. industry will suffer. "500 U.S. companies showed an increase in reported financial losses of 21 percent, or $455.8 million, in 2002," losses the authors attribute to commercial cyber warfare (Knapp & Boulton 2006, page 83).

Valeri and Knights (2000) second Knapp and Boulton's concerns about the vulnerabilities of U.S. military and civilian infrastructure. The authors seek to speculate about how terrorists will ultimately exercise Offensive Information Warfare (OIW). They argue that terrorists will focus on electronic commerce websites instead of national infrastructure, as the former will be significantly

more accessible and might ultimately wreak the most havoc across the nation. In addition, attacks on commercial industry will seriously damage consumer trust in the Internet, and might ultimately undermine governments' plans to convert services to the digital domain. Valeri and Knights concur with others about the consequences of low barriers to entry for cyber warfare, "the skills to carry out OIW are easily available as the Internet and exposure to information and network technologies encourages increasing technological sophistication in society" (Valeri & Knights 2000, page 20).

John Arquilla and David Ronfeldt (1999) establish a new subfield of cyber warfare, which they call Netwar. "Whereas cyberwar usually pits formal military forces against each other, Netwar is more likely to involve non-state, paramilitary, and irregular forces. To be more precise, the term Netwar refers to an emerging mode of conflict (and crime) at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age." (Arquilla & Ronfeldt 1999, page 194). Arquilla and Ronfeldt note that the term "cyberwar" has become misleading with the advent of newer technology. However, while Netwar and traditional cyberwar differ in their respective forms, Arquilla and Ronfeldt conclude that both are potentially catastrophic threats.

2.2 The Attribution Problem and International Law

The internet facilitates anonymity. A number of researchers have highlighted attribution as one of the most menacing aspects of cyberwar. Clark and Landau (2011) claim that deterrence becomes exceptionally difficult with the comparatively higher level of anonymity in cyber-warfare. "Retaliation requires knowing with full certainty who the attackers are" (Clark & Landau 2011, page 2).[3] Similarly, Libicki (2009) argues that the internet may well pose an intractable problem in terms of deterence. "The calculus of deterrence is fairly straightforward: The lower the odds of getting caught, the higher the penalty required to convince potential attackers that what they might achieve is not worth the cost" (Libicki 2009, page 43). Attackers are more likely to strike if they are less likely to be targeted in return by countries or groups subject to cyber aggression.

[3]This is simply not true. Certainly, retaliation improves with information about perpetrators, but blanket retaliation can also prove effective, if those responsible are included among those punished. Authorities seldom possess the benefit of "full certainty" in any context. The U.S. domestic standard is merely better than a "reasonable doubt."

Again the focus is on the potential for harm, while ignoring the motives and operational logic of perpetrators. If internet anonymity is awkward for targets of attacks, it is certainly also a problem for initiators. Terrorists spend as much time trying to market their exploits as they do fighting, bombing, assassinating, etc. Where anonymity protects an aggressor from retribution, it also dilutes credit for the deed. Vandals often "tag" their handiwork — creating an identity where none need exist — precisely because anonymity has both advantages and drawbacks. Internet vandals also brand their exploits, presumably in an effort to counteract, rather than maximize, anonymity.

Just as ongoing cyber attacks from unidentified sources do not give the target a way to retaliate, they also do not give the target a ready way to accommodate an attacker's demands. Demands from an anonymous cyber warrior will tend to be ignored or reneged on, once vulnerabilities are identified and addressed. Demands might also come from a source that did not, or even was not capable of, mounting a cyber attack. As with the use of identifying symbols in war, it is in the interest of the attacker to "brand" its efforts in order to elicit concessions from a target. Indeed, even if demands are complied with, it will be difficult for an attacker to obtain sustained compliance, given the impossibility of demonstrating future capabilities and the temporary nature of harm.

Discussion of attribution problems in cyber space also reflects a subtle but telling shift in framing. Libicki's simple calculus of deterrence, for example, involves "getting caught," something more often characteristic of crime than war. Some aspects of international relations involve anonymity. Espionage, covert operations and certain kinds of political theft or murder function most effectively when the perpetrators are unknown, or indeed when the operations themselves remain undisclosed. Strategic or tactical advantage can also stem from anonymity and surprise in terrestrial military missions, though nations and groups often sacrifice surprise and advertise their role in contests in order to exercise advantages in the form of foreign concessions or tacit or formal admission of defeat. How does one surrender to no one in particular? The advantage of anonymity will persist for peripheral forms of warfare on the internet, just as it has played a role in terrestrial competition and conflict. But most forms of warfare or potential warfare actually invite disclosure of an initiator's identity. As I have already noted, coercion requires attribution, not of the target but by the initiator. Similarly, threats designed to elicit concessions or deter aggression are already

problematic in physical space (Powell 1990, Nalebuff 1991). This "credibility problem" mirrors the attribution problem and is likely to make internet aggression all the more problematic for initiators.

In addition to the attribution problem, several scholars note that cyberwar creates an unparalleled legal environment, one in which even defining the scope of activities has become problematic. The relatively recent emergence of cyber warfare means that nations have not yet had time (or perhaps the ability) to solidify the legal standing of cyber conflict in international law. Charles J. Dunlap Jr. (2011) notes that democracies in particular have sidestepped previous attempts to formulate a treaty. Indeed, it is inherently difficult to legally define a process when capabilities have yet to be uncovered. Cyber attacks must be looked upon as the legal equivalent to armed attacks (Cerf 2011). Yet, as Schmitt notes, the legal definition of armed conflict involves "significantly destructive attacks taking place over some period of time and conducted by a group that is well-organized" (Schmitt 2010, page 176), something that has yet to clearly manifest in cyberspace.

2.3 Cyber Salience – A Balancing of Perspectives

While the bulk of reactions to cyberwar have emphasized dramatic potential pitfalls for developed nations and the United States in particular, some studies attempt to provide a more balanced perspective. Tim Maurer contrasts the gloomy picture offered by Clarke and Knake with the likely determinants of loss of life associated with a cyber attack (Maurer 2011). Maurer lists these determinants as the relative security of civilian infrastructure, participation of non-state actors, and the evolution of law regarding retaliation strategies. Will a state be allowed to respond to a virtual attack with kinetic warfare, for example? Maurer concludes that loss of life from cyber attacks will generally be slight, "a digital Pearl Harbor would cost fewer lives than the attack 70 years ago. It might not be pretty, but from a humanitarian point of view, that's good news" (Maurer 2011).

Wesley Clark and Peter Levin (2009) anticipate an inevitable rise in cyber-warfare, one that will eventually involve broad sectors of society. Western nations will face "network-born disruptions of critical national infrastructure" — including terrestrial and airborne traffic, energy generation and distribution and the U.S. financial system. However, the authors note that the United States and other nations are doing a great deal to mitigate the threat. The United States has pledged a reported

$30 billion by 2015 as part of the Comprehensive National Cyber Security Initiative. In addition, Clark and Levin note lessons learned from previous attacks. The most effective electronic security strategy must operate under full disclosure. Experts in academic, industrial and governmental sectors must quickly collaborate on a mitigation strategy. Yet, Clark and Levin also acknowledge that "electronic security works best when it is autonomous, adaptable, distributed and diversified."

Before working on eliminating the cyber-threat, Stephen Walt (2010) argues that one must define the different elements of the dangers grouped under the common rubric of "cyber-warfare." For Walt, cyber-warfare consists of four distinct issues: degrading an enemy's military capabilities, penetrating networks to shut down civilian infrastructure, web-based criminal activity, and cyber-espionage. These four issues help put cyber-warfare in perspective as Walt calls for a comparative cost-benefit analysis. Is a hacker more likely to crash a power grid than is a blizzard? Does focusing on eliminating cyber-espionage make way for increased success with traditional forms of espionage?

In a similar vein, Thomas Rid (2012) argues that cyberwar is not really war because it fails to conform to conventional definitions of conflict. Rid's chief point — mirroring in an interesting manner Maurer's argument — is that cyberwar is not sufficiently violent or casualty-producing to be considered war. As such, cyberwar is a misnomer. However, this point risks being purely academic if cyber conflict supplants military violence as the ultimate arbiter of international politics. Cyberwar does not need to be war to make war obsolete. Instead, it must fulfill the existing functions of terrestrial warfare if it is to rival the utility of existing forms of conflict. As I argue below, the internet is extremely unlikely to substitute for, or serve as an alternative to, earthbound warfare.

3 Contrasting Vulnerability and the Nature of Threats

The notion that cyberspace is a new domain where old rules don't apply and where omnipresent vulnerabilities require extensive (and expensive) military reform is both intuitive and widely expressed. Cyberspace *could* constitute a hidden back door, enabling opponents to undermine U.S. national security and circumvent the terrestrial advantages of the existing western-dominated order. History makes clear that technological innovations or new modes of organization eventually topple

every hierarchy.[4] However, it is far from clear that we are in the midst of such a transition today. Lacking information about whether developments are transformational or merely incremental, it may make sense to begin with a few guidelines about when panic is in order, and when it is not. A reasonable level of caution is probably provided by common sense. Most readers will lock their doors at night, for example, and refrain from handling large sums of cash in dark alleyways. Imagining what others *could* do to harm each of us, however, can quickly slide into paranoia. It is not reasonable caution to believe that someone is intent on mischief simply because harm is possible.

Even in the safest of societies, individuals, groups and entire communities are subject to an enormous variety of potential hazards. Much could be done to damage each of us, even though few of these possibilities are actually exercised, or experienced, with any regularity. The physical world hosts a multitude of venues for extremely unlikely accident or disease. A small number of people prefer to stay in their homes rather than risk being struck by lightening or struck down by botchulism. Still, individuals with these concerns often receive more attention from psychiatric professionals than from military planners. Being vulnerable should be novel to no one living in the modern world. Indeed, the capacity to harm in a highly integrated world is so ubiquitous that blood would coat the streets if it were not for the fact that relatively little relationship exists between the capacity to attack and the actual prospect that one is invaded, assaulted or otherwise done in.[5]

Just about anything is possible. Someone may have poisoned your morning *Corn Flakes*. Terrorists may have singled you out for vengeance, or you might just become one of the unlucky few who are in the wrong place at the wrong time. When a commuter steps outside to start her car or to catch the bus, it is impossible to be certain that no truck will jump the curb and that every asteroid will remain in the heavens. And yet, despite endless possibilities for damage or death, the vast majority of us have yet to harden our living rooms against cruise missiles or falling satellites. In dealing with known unknowns, we became comfortable with the fact that we are unprotected. Few homeowners in California carry earthquake insurance, for example, though it is by no means impossible that "the big one" will strike tomorrow. We do so because security itself has a price;

[4] See Gilpin (1981), McNeill (1984), van Creveld (1989), Goldman & Eliason (2003) and Lieber (2005) for discussion.

[5] The current fascination with vampires (popular) and zombies (academic) illustrates the basic point. Aggression becomes endemic if harm has an intrinsic payoff (e.g., human beings are food). Vampires and zombies threaten not just individuals but civil society since interdependence/specialization requires that vulnerability not equal insecurity.

protection from unlikely events is literally not worth the effort. One could buy that bulletproof vest relentlessly listed on Ebay, but then how often would it really be proper attire at the office or in the classroom? Unlike possibilities, the probabilities of esoteric catastrophe are by their nature minute. Unlikely events are unlikely, and so most of us go about our business, without paying undue attention to the potential menace from the skies or, for that matter, from our fellow citizens.

Governments face similar realities. Many threats are conceivable, but few are likely to occur. All forms of security involve assessing risks and allocating limited resources to address tractable threats, making the largest (finite) improvements in protection or, conversely, the greatest increases in influence.[6] Every dollar spent on national defense must be taken from objectives like education, infrastructure, or paying down the debt. Only extremely affluent (or paranoid) populations pay the price of pursuing protection from the most exotic hazards. More to the point, protection is inevitably incomplete, and comes with its own consequences, including other forms of insecurity. The risk of attack is never zero, since a potent defense or deterrent endangers the security of others.[7]

If violence is a perennial possibility, why don't human beings live in consummate fear? Most of us are safe because the multitudes who are capable of causing us harm have little interest in doing so. For the most part, violence does little that potential perpetrators view as worth their while. Much of humanity is protected by an invisible shell of indifference or inefficaciousness. The stranger coming toward you on a busy city street could easily swing out his arm at the last minute, catching you under the chin. He could be carrying an Uzi, which in a fit of rage will leave you and other passersby on the pavement in a pool of intermingling body fluids. We see little such violence because it does little to benefit the violator, just as bludgeoning the odd shopper in the mall fails to profit the bludgeoner. Violence is costly, risky, and mostly unproductive. When we learn of violence, our natural inclination is to ask "why?" Like a police detective, we seek a motive. When on occasion violence occurs with no apparent logic as to target, it is remarkable, and puzzling.

Most of us are capable of seriously damaging others, but for the most part we fail to exercise our capabilities because there is no positive reason to strike. The mere capacity to inflict harm

[6]The distinction between security and influence is often missed or mis-represented in popular discussions of defense. For the most part, for example, debates in the United States center on security, while in fact much of the U.S. defense budget is devoted to obtaining/maintaining international influence. Indeed, the two are frequently substitutes.

[7]This is enshrined in the security dilemma. See, Herz (1950), Jervis (1978), Schweller (1996) and Glaser (1997).

is thus not a very good predictor of aggressive behavior. Because few of us are likely to be the target of an attack, each of us can greet each day with minimal anxiety, to say nothing of personal security, not because we are effectively protected from harm, but because harm is inconvenient, unnecessary or pointless for potential perpetrators. Attacking us (or others) serves no purpose.

The internet makes it possible to interact with people just about anywhere on the globe as easily, or even more easily, than conversing with the neighbors next door. Initial attention to the mobility of cyberspace focused on the potential for good, but convenience also overcomes natural barriers to conflict. The supply of targets for cyber acts of aggression is certainly huge relative to the supply of perpetrators of physical violence. Viewed in this way, it is remarkable that cyber space is not predominantly the domain of fraud, identity theft, and other acts of predation, interspersed only by porn and the occasional Nigerian emailer looking to deposit millions in your bank account. Yet, if the internet makes it easy to reach out and touch others, it in no way makes those contacts profound. Casual attempts to undermine your welfare abound, but it is with equal casualness that we ignore the bulk of spam, or internet sites marketing lapsed software. Predation continues unabated on the world wide web, but if it is easy to reach us, contact is all the more superficial.

The ease of contact is generally inversely related to the prevalence of transgression. Just as a pedestrian can be fairly comfortable walking in front of a stopped vehicle at an intersection, most internet traffic is benign, simply because perpetrators are rare and opportunities are many. Cyber space has not made life more dangerous for the multitudes. There are crimes on the internet, but it is far from clear that the internet has increased overall criminal behavior. Internet crime often substitutes for crimes that would otherwise have been committed in real space. Perhaps even more to the point, much of internet fraud and cyber violence is intrinsically tied to the physical domain; much of the harm initiated on the internet eventually gets perpetrated in more conventional ways.

The safety that mass populations achieve from their numbers and anonymity in terms of targeting is denied political institutions and their representatives. Countries and organizations have facilities and personnel that can be targeted with violence. How might the ability to strike institutions and infrastructure change the risk of cyber attack? Once again, we must inquire not about what could happen but why individuals, groups or nations might be motivated to take action.

Nations and organizations can be attacked through the internet, just as they have long been attacked in physical space. The ease with which such attacks can be perpetrated are an obvious, and much discussed, phenomenon. Physical space has always been an important barrier to conflict.[8] Even today, the single best predictor of interstate conflict is the contiguity of national borders (Hensel 2000, Senese 2005). However, lowering the cost of transmission of an attack is only synonymous with increasing the appeal of a given approach to war if the approach is also effective in achieving certain ends. Beyond being anonymous and a multitude, the main thing that protects individuals from all types of violence is even more potent for political institutions; it is not clear in many cases how force will yield a change in the tide of the affairs of states or organizations. Cyber attacks can be appealing as political acts only to the degree that they affect the decisions organizations and sovereigns make with and without cyber violence. Since understanding when and how cyberwar influences politics is largely identical to understanding how conventional forms of military violence act upon politics, I turn next to an analysis of the nature of terrestrial warfare.

4 War and Peace in the Internet Age

U.S. Defense Secretary Panetta's warning that "the next Pearl Harbor" could well occur over the internet appears designed to evoke strong emotions, rather than prompt clear thinking about the likely nature and limitations of cyberwar. No event in the twentieth century did more to realign U.S. public opinion, mobilizing the nation psychologically for entry into the Second World War. The analogy may in fact be apt, but almost certainly not in the manner imagined by the Secretary. The situation in 1941 actually serves as a useful point of comparison with a surprise internet attack. To understand why a cyber Pearl Harbor is not as threatening as it sounds, it will help to review what the air raids on December 7, 1941 were meant to accomplish and what they actually achieved.

Before diving into Panetta's Pearl Harbor analogy, however, I first discuss the nature of war and how key attributes of warfare (mal)function over the internet. Nations and non-state actors make war to further their interests when incompatibilities exist between those interests, and when

[8] Boulding (1962) championed the so called "loss of strength gradient," whereby power attenuates with distance. Buhaug & Gleditsch (2006) show that the relationship, though weaker today, remains in effect to the present time.

alternative methods of conflict resolution are deemed inefficient or ineffective. While many conflicts are conceivable, most do not occur precisely because prospective participants recognize that threats or uses of force are futile, violence often cannot achieve the objectives for which nations strive. If futility is a problem for terrestrial conflict, it is an even more encompassing barrier to cyberwar.

4.1 A (Very Brief) Logic of War

The theory of war provides two basic mechanisms for the expression of political interests through physical violence. First, force can be used to punish or compel, indirectly affecting the state of the world by harming an enemy to make it do something that the enemy would not do otherwise, or alternately discouraging change by raising the price of aggression. Just about everyone from parents, to police and prime ministers seems to grasp the intuition behind creating consequences in order to modify behavior. Second, force can be used to conquer, directly imposing one's will on another by capturing and controlling inhabitants or resources contained in a given physical space. One thing that the recent "Occupy" movement shared with the U.S. military was the conviction that denial can prove effective if exercised for a sufficient period of time.[9] The ability to conquer or compel can in turn be used to achieve these objectives through actual force (offense or defense), overt threats (deterrence or compellence), or the shadow of war (e.g. diplomacy) (Blainey 1973, Fearon 1995).

During the Cold War, the two superpowers could easily have annihilated one another, along with much of the rest of the world, given vast nuclear arsenals. Yet, these capabilities were not exercised directly and the prospect of mutual harm even led to the peculiar stability of MAD. Again, the mere capacity to hurt tells us relatively little about the actual advent of violence, even though the potential in the Cold War was extraordinary and mutual assured destruction by its nature meant that devastation could not be prevented. Indeed, it was this mutual ability to attack, and mutual inability to defend, that many credit with Cold War stability (Mearsheimer 1983, Waltz 1990).

In contrast, Japan kept even its own diplomats in the dark about its plans to attack U.S. bases in the Philippines and Hawaii precisely because it could not share information about its intentions with

[9]The whole question of denial/conquest is whether a target is likely to acquiesce. The British have occupied Scotland for centuries, with some success. They occupied Ireland for just about the same length of time with very little lasting political effect. Perhaps days or decades are unlikely to succeed when centuries often prove insufficient.

U.S. officials without fatally weakening the effectiveness of such a plan (Slantchev 2010, Gartzke 2006). Nixon reportedly threatened to restart the "Christmas" bombing campaign of Hanoi to expedite the forging of a settlement ending U.S. involvement in the Vietnam Conflict. The threat could be made under any circumstances, but it was more credible given that Hanoi had recently been attacked and the consequences of renewed heavy bombing were also clear. Whether force is threatened or carried out depends on whether threats can be made without degrading instruments of military advantage. Revelation of the ability to harm can prove sufficiently compelling to cause a target to make concessions or to alter the target's behavior. Conversely, if threatening an enemy makes an eventual attack less effective, then the temptation may be to strike rather than threaten.

Perhaps with reason, but not with considerable clarity, experts on cyber security have failed draw the same conclusions from the inability to protect that strategists drew from the Cold War. Mutual assured destruction may not exist in cyberspace, as it did in the terrestrial world of the 1950s through early 1990s. However, what remains to be explained is why the internet is such a different strategic setting, and what this means for what nations can and cannot accomplish, both in terms of deterrence and compellence. Indeed, while the Cold War is remembered as the ideal deterrence environment, strategic thinkers and government officials struggled with how they could exercise influence in such a world. The mere potential for imposing harm did not imply that harm would be imposed, or even that, when imposed or threatened, nations would respond in an obliging manner. Few could doubt in retrospect that citizens and leaders on both sides of the iron curtain felt vulnerable, especially during the early years of the post-World War II period. It does not follow, however, that a heightened sense of insecurity was reflected in actual behavioral conflict. Whether warfare in the cyber era will depart radically from previous patterns, or will mimic, in part or in whole, conflictual politics from earlier eras, will depend on the degree to which the strategic logic of cyberwar accommodates the objectives of political actors in contemplating or exercising coercion.

Nor do students of cyberwar seem much concerned with implications of Nixon's Hanoi bombing campaign. The threatened use of force in this, and most other instances, is intended to alter behavior through the prospect of long-term damage. To the degree that harm can be quickly and easily repaired, there is not much leverage in such threats. Conversely, details injurious to attackers

or to the effectiveness or potency of an attack are typically concealed from an opponent, even when this information would significantly increase the credibility of coercive threats. Flight plans, bomb loads and electronic countermeasures used by U.S. B-52s, for example, were not shared with Hanoi, since this would have deeply compromised the capacity of U.S. forces to carry out Nixon's threat.

Nations, groups or individuals with the ability to inflict harm must ask, not just how much can be inflicted at what cost, but also what is to be achieved through force, and whether these ends are justified in terms of price and availability of alternative, typically cheaper, mechanisms. Force, or the threat of force, is useful as punishment to the degree that the harm imposed is substantial and durable. Damage that can be quickly or easily undone will not do much to deter or compel, but it will alert an enemy to vulnerabilities, and also antagonize an opponent, increasing the danger of counter attack and/or future opposition. The threat or realization of physical conquest can be effective provided the perpetrator finds it worthwhile to engage in the costliest form of politics. Here again, the simple ability to act aggressively is not itself sufficient to rationalize or predict aggression. The United States could probably conquer Canada if it chose to, and yet Canada remains (by all accounts) sovereign and independent. Most states, groups and individuals persist in peace because they can conceive of no benefit from force, even if violence, and victory, are feasible. The fact that harm can be propagated over the internet does not suffice to predict that cyberwar will become a substitute for terrestrial conflict, or even that it will be an important domain of future warfare.

4.2 Warfare in Cyberspace

Beyond questions of means and motive, two basic features make cyber warfare different from other types of conflict. First, the bulk of damage contemplated by cyberwar is in all likelihood temporary. The assumption among many cyber-pessimists that the potential for creating harm is sufficient to make cyber space a suitable substitute for, or at least an alternative to, terrestrial conflict is simply incorrect. Shutting down the power grid, or preventing communication could be tremendously costly, but most such damage can be corrected quickly and with comparatively modest investment of tangible resources. Regardless, damage of this type is sunk. Losses experienced over a given time interval cannot be recovered whatever one's reactions and so should not have much direct impact

on subsequent policy behavior. Harm inflicted over the internet or through any other medium will matter politically when it involves changes to the subsequent balance of power, or when it indicates enemy capabilities that must be taken into account in future plans. Precisely because cyberwar does not involve bombing cities or devastating armored columns, the damage inflicted will have a short-term impact on targets.[10] To accomplish meaningful objectives, cyber attacks must contribute to other aspects of a more conventional war effort. In order to affect the long-term balance-of-power, for instance, cyberwar must be joined to other, more traditional, forms of war.

Temporary damage can be useful in two circumstances. First, compromising or incapacitating networks might afford an enemy valuable tactical, or even strategic, advantages. An opponent that cannot shoot, move, resupply or communicate will be easier to defeat. However, this still requires the advantaged party to act through some medium of combat to seize the initiative. Notions that cyber attacks will themselves prove pivotal in future war are reminiscent of World War I artillery barrages that cleared enemy trenches, but which still required the infantry and other arms to achieve a breakout. Whether an actor can benefit from cyberwar depends almost entirely on whether the actor is willing and able to combine a cyber attack with some other method — typically kinetic warfare — that can convert temporary advantages achieved over the internet into a lasting blow. Internet attacks thus offer an assailant a "soft kill" that is valuable only when attackers intend and prosecute follow-on attacks with traditional military force to permanently weaken an enemy.[11]

The notion of a devastating surprise attack is a particularly baroque aspect of cyberwar paranoia, and is certainly frightening to the degree that such scenarios are accurate. However, the idea of a surprise attack over the internet is in fact extremely misleading and relies on a fundamental misconception of the role of internet-based aggression. It has seldom been the case in modern times that any one element of combat proves pivotal. Instead, it is the ability to combine elements into a complex whole that increasingly distinguishes adept utilization of military force (Biddle 2004).

The archetype of modern, combined arms warfare is the *blitzkreig*, where the lethality and effectiveness of conventional military violence is enhanced by actions designed to disrupt the enemy's

[10] In the 1970s the so-called neutron bomb promised high casualties with minimal damage to physical structures. It might be tempting to think of cyber weapons as anti-neutron bombs, since they damage infrastructure, leaving people largely unharmed. Yet, this is also a key limitation of cyberwar, as damage is temporary and far from complete.

[11] Non-lethal weapons have similar functionality. Immobilizing an enemy with sticky foam works until it doesn't.

military and civilian infrastructure. An important element of *blitzkreig* was the use of terror weapons, such as the Ju 87 "Stuka" dive bomber, to sow panic, mobilizing enemy populations to flood roads and railways, thereby crippling infrastructure needed by the defense. Yet, fear is temporary and in the absence of substance, quickly subsides. The Stukas were effective only as long as Germany held other military advantages over its enemies. Unless threatened with immediate invasion, the terror role of the Stuka was largely redundant. Stukas contributed little to Germany's attempt to subdue the United Kingdom, for example. Stuka units experienced heavy casualties against a competent air defense and had to be removed from service in the Battle of Britain. The hubris of Luftwaffe commander Göring in promising victory while exploiting only a single domain (the air) was precisely that he exaggerated the independent effect of a new technology on war.

There is no reason to believe that cyberwar will be any more useful as an isolated instrument of coercive foreign policy. An attack that causes temporary harm will inevitably be followed by countermeasures and heightened vigilance, as has happened for example in Estonia in the aftermath of the 2007 attacks. For cyber aggression to have lasting effects, a virtual attack must be combined with physical intervention. Knocking out communications or power infrastructure could cause tremendous disruption, but the ability to quickly recover from such attacks implies that the consequences in terms of the balance of national power would be negligible. The need to follow virtual force with physical force in order to achieve lasting political effects suggests that the application of cyber warfare independent of conventional forms of warfare will be of tertiary importance in strategic and grand strategic terms. If one cannot foresee circumstances where physical aggression is plausible independent of cyberwar, then cyberwar is also unlikely to constitute a critical threat.

A second element of the logic of cyberwar has to do with influence. Rather than attacking directly, an actor can use the potential to harm (deterrence or compellence). The ability to shut down the U.S. energy grid, say, might be used to compel U.S. officials to refrain from aggressive policies or actions, or to persuade the United States to make diplomatic concessions. Yet, the problem with the standard deterrence or compellence logic in the context of potential cyber attacks, as I have already pointed out, is that revealing a given set of cyber capabilities heavily degrades their usefulness. Deterrence or compellence are therefore marginal as "pure" actions in cyberspace.

Indeed, concerns that nations will not be able to deter cyber aggression amount to a recognition that neither will cyber threats prove very effective as threats or inducements. Again, actions in cyberspace can be combined with initiatives in physical space, but this just reinforces the fact that, rather than a distinct form of conflict, cyberwar is basically tied to conventional forms of warfare.

Imagine for a moment that a foreign power has hacked into the communications systems of the United States or another major western power. Imagine further that this foreign power can disable cell phone communication, or military radio networks more-or-less at will. The foreign power could threaten its target with this capability, but obviously the leadership of the target state must be skeptical of such a threat, since the foreign power could easily be bluffing. Proof of the capacity to damage the target nation is needed, but such evidence would in turn jeopardize the effectiveness of the cyber attack, allowing the target to address vulnerabilities, or adopt countermeasures.

Contrast this with the U.S. revelation in the 1990s that it had developed radar-evading "stealth" aircraft. Knowledge by foreign powers that a confrontation with the United States would necessarily involve the risk of attack by stealthy strike fighters and bombers in no significant way lessened the military effectiveness of these weapons systems, since countermeasures to stealth technology have been slow to develop. Stealth thus serves as an excellent deterrent/compellent, since the technology can be used to coerce an opponent without sacrificing much of its military value. The "perishable" nature of offensive capabilities in cyberwar mean that advantages offer only a very limited potential for deterrent or compellent threats, and thus create little in the way of leverage for countries that have, or plan to invest in, cyberwar assets. Deterrent/compellent threats work best when they are tied to capabilities that are not much affected by knowledge of the capabilities, while the opposite is true for capabilities that are compromised by revelation of forces, technologies or attack plans.

Offensive cyber advantages are thus "use and lose" capabilities. Revealing the capacity to harm via the internet typically also means tipping the enemy off to vulnerabilities that can be addressed, while inflicting harm does not have a durable effect on the balance of power. "Use and lose" capabilities cannot compel or deter, since convincing evidence of the capacity to harm is itself useful in nullifying the threat. If instead cyberwar is waged rather than threatened, then cyber attacks remain adjunct to terrestrial force unless they permanently alter the balance of power.

4.3 The Myth of a Cyber Pearl Harbor

The air strikes on December 7, 1941 against U.S. military instillations in Hawaii and in the Philippines were an important tactical and even strategic victory for Japan. Yet, the attacks were clearly a failure in grand strategic terms, setting up a nearly inexorable path to Japanese surrender.[12] Officials on both sides recognized this almost immediately. Admiral Isoroku Yamamoto is said to have offered the starkest commentary, "all we have done is to awaken a sleeping giant and fill him with a terrible resolve."[13] For its part, the United States could not be bothered to give war in the Pacific top billing, focusing much of its recourses, personnel and attention on the war in Europe.

The Japanese decision to go to war had been a calculated gamble, balancing the imperatives of seasonal weather patterns and the impending decline in power projection capabilities for the resource-starved Empire with the realization that much was being staked on a complex plan linking the conquest of the oilfields of Southeast Asia with a temporary shift in the regional balance of power in the Pacific (Morton 2000). With almost no indigenous sources of iron, rubber or especially oil, Japan was dependent on foreign-held reserves to feed its factories and allow it to sustain its occupation of Manchuria and parts of China. The U.S. embargo led Japanese officials to consider stark alternatives. Either Japan must relent and withdraw its forces from East Asia, or it would have to capture oil-rich regions in the South. This in turn put Japan in direct conflict with the United States. The Japanese plan was to blunt U.S. naval and military capabilities temporarily, long enough to present the United States with a *fait accompli* and create a defense in depth in the western Pacific that would force the United States to accept a negotiated settlement of the war.

The prospect of significant relative decline and optimism about the potential benefits of a temporary shift in power in the region were critical elements of Japan's decision to go to war. Importantly, Japan underestimated the psychological impact that the Pearl Harbor raid would have in mobilizing U.S. public support for the war. They also overestimated the damage that they could inflict on U.S. forces.[14] The surprise assault famously failed to catch the U.S. aircraft

[12] "From a strategic point of view, Pearl Harbor was one of the most spectacular miscalculations in history" Ian W. Toll, The New York Times op-ed, December 6, 2011.

[13] Documentary evidence for the quotation is unavailable, though it certainly summarizes Yamamoto's views.

[14] Evidence of this is reflected in subsequent efforts by the Imperial Japanese Navy to realize their original objective. Midway, in particular, was an elaborate trap, masterminded by Yamamoto, to locate and destroy the U.S. carrier

carriers in port. It was this inability to impair U.S. naval airpower that vexed Yamamoto and other Japanese commanders most. Even allowing for optimism and error, however, Japanese leaders were reluctant to contemplate war with the United States prior to the end of 1940, when events in Europe laid bare Dutch holdings in Asia and dramatically weakened the ability of British forces to resist.

Tactical or strategic surprise is useful as a temporary force multiplier; an attack such as that on U.S. and allied forces in December 1941 could shift the balance of power in Japan's favor for a time, but the real value of a surprise attack is what else it may allow an assailant to accomplish. An attacker can exploit the effect of surprise to prepare a more effective defense or, alternately, to prosecute further offensive action against the target of the surprise attack or others. A surprise attack has limited utility in isolation, precisely because the effect of surprise fades with time.

Japanese war planners anticipated the temporal nature of advantages gleaned from the surprise attacks on Pearl and elsewhere. It was hoped that Japan could secure needed resources in the South, fortify its gains in depth, and wait out the American onslaught.[15] At no time did Japanese officials look forward to unlimited war with the United States. Indeed, Japanese planners recognized the impossibility of defeating the United States on its own territory.[16] In the months after December 7, the United States mainland was open to attack. Japanese forces landed in the Aleutian Islands and Japanese submarines shelled a few isolated coastal communities in California, Oregon and Canada. However, there were never any serious plans to carry the war to the continental United States.[17]

Now imagine that Japanese officials recognized from the outset that they would not be able to target the U.S. carriers or other U.S. military assets for permanent destruction. Instead, suppose (not very plausibly) that Japanese dive bombers and torpedo planes were fitted with special "delay bombs" that, unlike delay fuses, would simply disable a ship for hours, days, or possibly weeks, rather than permanently, or at least for months or years. Faced with this (altered) reality, Japanese officials and military planners would have been forced to contemplate a very different war, one that

force. See, Prange (1983); Fuchida (1986); Parshall & Tully (2007) and Symonds (2011).

[15] "Japan planned to fight a war of limited objectives and, having gained what it wanted, expected to negotiate for a favorable settlement" (Morton 2000, page 110).

[16] Admiral Yamamotos other famous quotation, which was meant as an ironic reference to total war with the United States, notes that "To make victory certain, we would have to march into Washington and dictate the terms of peace in the White House." Yamamotos letter to Ryoichi Sasakawa is quoted in Prange (1981, page 11).

[17] Even the invasion of the Aleutians was later found to be a feint to distract attention from the attack on Midway.

they would almost certainly have preferred not to initiate. In effect, Japan would have had to choose to precipitate total war, as the surprise attacks themselves would not do much to diminish or delay a military response from the United States. The only value one could anticipate from a surprise attack, then, would be if one was able to follow up the attack with an invasion of the United States mainland. This is the basic shortcoming of cyberwar. Because cyber attacks involve "soft kills" of a target's military capabilities and civilian infrastructure, the point of the attack is largely nullified if an attacker cannot reasonably be expected to accompany internet aggression with terrestrial strikes designed to make permanent short-term damage to a target's security capabilities.

No foreign military force is capable of subduing the United States, now or in the foreseeable future, even with the assistance of a phenomenally successful coordinated cyber attack. If cyberwar is unlikely to allow a foreign power to permanently overtake U.S. or allied capabilities, and if temporary damage is only useful in conjunction with more conventional military operations, then an opponent must plan and evaluate its use of cyberwar in terms of its complementarity to terrestrial combat, not as an alternative method of force. If instead a cyber attack is carried out in which conventional force is either ineffective or not contemplated, then such an attack serves no purpose in grand strategic terms, degrading neither the target's permanent capabilities nor its resolve.

Unless cyberwar can substitute for a physical surprise attack, there is no reason to believe that it will be used in place of conventional modes of warfare. Nor is it clear why an attacker would choose to strike over the internet, unless a conventional surprise attack is also planned and when it is expected that the combination of cyber and terrestrial aggression will yield a decisive advantage to the attacker. If it is difficult to imagine a particular nation being attacked by traditional methods of warfare, even with the benefit of surprise, then it is hard to see how that nation might be fundamentally threatened by war over the internet. Indeed, the connection between internet aggression and traditional forms of military force imply a surprising prediction: cyberwar should be particularly appealing to capable states attacking weaker opponents. Rather than threatening to overturn the existing world order, cyberwar may perpetuate or even increase existing inequalities.

5 Additional Implications of Cyberwar

If cyberwar is unlikely to function as an independent domain, but as part of terrestrial military action, then the conventional military balance is the best indiction of where the most important threats exist in cyberspace. Thus, unless someone believes, for example, that economically and militarily advanced nations are in danger of physical attack from a foreign power, the threat of cyber attack cannot be treated as particularly serious in military terms, either. Most experts view the likelihood of an attack that subdues U.S. military capabilities and subjects the U.S. mainland to a foreign power as remote, even fanciful, for example. To the degree that this is so, it is not clear why U.S. officials or the public should fear the prospects of war conducted over the internet.

In fact, the states and entities that should be most concerned about cyberwar are the same states and non-state actors that are currently vulnerable to conventional terrestrial aggression. Cyberwar is not a revolution in military affairs in strategic (military) terms, nor is cyberwar likely to prove revolutionary in terms of existing global or regional power structures. Indeed, if anything, cyberwar appears to be reactionary, reinforcing the advantages of states that already possess significant terrestrial military advantages. The need to prosecute cyber attacks with more kinetic forms of force, and the perishability of cyber capabilities in the face of revelation mean that nations with capable militaries are best equipped to exploit temporary damage inflicted by cyber attacks, even as they are better able to credibly threaten cyber attacks and/or "reveal and replace" a target's vulnerabilities. This new mode of warfare, most feared by technologically advanced states, may actually pose greater grand-strategic challenges to the technologically backward or weak.

Though limited, available examples of cyberwar reinforce this counter-intuition. Attacks on Estonian websites, which appear to have originated from Russia, pitted a tiny nation against a considerable military and economic power. The ability of Russia to prosecute effects of the attack, not just on the internet but through military and diplomatic pressure, ensured that the impact was much more potent than if some non-aligned group of hackers carried out equivalent attacks. Similarly, the Stuxnet worm — initiated according to most sources by a U.S. intelligence agency — was more effective because of the military balance between the two powers than it would have been

if Iran had been able to counter with military action.[18] The Russian invasion of Georgia/South Ossetia is perhaps the clearest example of the kind of combined terrestrial-cyber contest anticipated here. As one commentator put it, "This appears to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains (consisting of Land, Air, Sea, and Space)" (Hollis 2011, page 2). It is under conditions where the conventional military balance already favors an attacker that cyber attacks are most efficacious.[19]

An open question exists in any crisis about how far competitors are willing to escalate, but an ability to counter cyber attack with other, more kinetic forms of military violence serves alternately to deter or to facilitate the use of cyber capabilities, giving those nations with terrestrial military power yet another option that, even if available to their opponents, may prove extraordinarily dangerous to practice. As we see today with U.S. drone attacks and special operations raids on foreign sovereign territory, the power to do much more ensures that an opponent maintains a level of discretion in its response to provocation. Few can doubt the reaction of the United States, for example, if Pakistan were to attempt to conduct a commando raid on U.S. territory. Nations that can physically punish others for transgressions in any domain, electronic or otherwise, are better able to operate in all domains. Once one distinguishes between simple vulnerability and actual threats, terrestrial capabilities become pivotal in determining who exercises cyber capabilities.

Even if cyber attacks are available to weaker actors, their effectiveness will be stymied where these actors lack the ability to prosecute advantages generated by cyberwar, and where weakness in more traditional modes of diplomatic, economic, and military competition ensure that these actors are exposed to countermeasures. The intractable nature of vulnerabilities ensure that cyberwar will not fundamentally transform either warfare or world affairs. Despite a dependence on high technology, developed nations will find that they are better able to exercise cyberwar as a political tool. Attacks against prosperous western powers, if well publicized and the source of considerable anxiety, will turn out to be epiphenomenal. While other forces may well transform contemporary hierarchies, cyberwar will most likely function to perpetuate existing inequalities of influence.

[18] For a detailed discussion of the politics and technical nature of Stuxnet, see Lindsay (2012).

[19] Sheldon (2011, pages 99-100) is skeptical that "cyberpower" will prove coercive, though this view depends heavily on the recent past, rather than a cohesive theory of the role of cybewar war in modern integrated military systems.

5.1 The Adjunct Role of Cyberwar

Because war on the internet is adjunct to more conventional forms of fighting, a cyber attack is extremely unlikely to prove pivotal in confrontations involving capable states or their partners. Still, cyberwar could be used by and against forces in the field and this is certainly an important concern. A common method for evaluating the implications of new technologies for war and peace involves the offense-defense balance. Proponents of offense-defense theory focus on material (Quester 1977, Hopf 1991, Glaser & Kaufmann 1998, Adams 2003) or cognitive/informational factors (Snyder 1984, Van Evera 1998) that they believe will lead to increased military aggression. Nations or time periods that experience or perceive offensive advantages will be associated with more war, while the opposite is said to happen when innovations or circumstances favor the defense. There is considerable skepticism about the empirical validity of offense-defense theory (Levy 1984, Gortzak, Haftel & Sweeney 2005), as well as about the ability of researchers to isolate factors leading to offense or defense dominance (Mearsheimer 1983, Shimshoni 1991).[20] Even if there were nothing controversial in the application of offense-defense theory, it would still be challenging to draw conclusions about the impact of cyberwar on the appeal of fighting generally, given that cyberwar is relatively untried, and given that cyberwar capabilities are not the only factors influencing the offense-defense balance. However, it is important in evaluating the impact of cyberwar to know whether the internet systematically favors attackers or defenders, and so I offer a few thoughts.

Jervis's (1978) original conception of instability induced by technology would seem well suited to explaining the effect of cyberwar on the probability of broader conflict among states. However, as Fearon (1998) makes clear, Jervis and other authors of offense-defense theory have failed to distinguish between advantages gleaned from initiating disputes, and those from acting aggressively, should war occur. Fearon (1998) also notes a more general tendency to confuse the shifting offense-defense balance with changes in the balance of power. Offense dominance implies that states are more likely to prefer to attack rather than defend, *ceteris paribus*, once one takes into account the prevailing balance of forces. A much weaker state is unlikely to prevail under any circumstances.

Imagine first that cyberwar is defense dominant. This does not seem likely and contradicts the

[20] For a rebuttal of these critiques, see Lynn-Jones (1995). Adams (2003) offers support for offense-defense theory.

prevailing view in the literature. Still, suppose for a moment that information infrastructures are more readily defended than attacked. In such as world, the balance of power would favor those states that could most effectively orchestrate military command, communications, logistics and intelligence through the internet and similar types of networks. Even if this imagined cyber world is defense dominant, however, it does not follow that terrestrial conflict is also defense dominant. The relative immunity of networks to attack could lead to a reluctance to use conventional force, or it could increase incentives to act aggressively, depending on whether secure networks are more critical for defenders or attackers. The standard military answer is that command and control are more critical for the offense, as commenders need direct control of their forces in the attack. If so, then perhaps defense dominance in cyber space is actually a bad thing, since it increases the appeal of attacking and (slightly) decreases the ability of defenders to prevail. Conversely, if as many contend, cyber space is offense dominant, then this would tend to weaken offensive operations in the physical world, making terrestrial conflict more defense dominant (or less offense dominant).[21]

The proposed conception assumes dichotomous conditions of network vulnerability that of course fail to reflect the dynamism that occurs during wartime. It may take time to disable networks. If so, then there is a first mover advantage that could prove more critical than the defense dominance created by the heightened need for attackers to conduct C^4I. Advantages may follow from an early start in cyberwar. Striking first could also be particularly valuable if disabling an opponent's internet also reduces an enemy's ability to retaliate. Since a state projecting power abroad benefits from being able to choose the time and place of attack, it might be that the first strike advantage in cyber space is more important than the pacifying effect of cyber offense dominance.

Regardless of whether the internet increases or decreases incentives to attack, it is very likely that cyberwar will continue to favor the strong against the weak. This is not to say that cyber attacks would have no effect, only that they are extremely unlikely to prove strategically decisive. A capability to address cyber threats is then useful, but planning for cyber warfare must be conducted within the larger framework of recognition that these capabilities are not in fact a "game changer."

[21] I am grateful to Eugene Gholz who initially raised the general question of offense and defense cyber dominance.

5.2 Cyber Terrorism

The events of September 11, 2001 animated the specter of insecurity in the western world; how are governments to protect their citizens in an age where the enemy is concealed and where an attack may come at any time or place? The temptation has been both to treat terrorism as an existential threat (because it is frightening) and to assume that the best response is a vigorous defense. Yet, as we have seen, one of the most effective mechanisms of protection is not to remove capabilities, but to puncture resolve, first and foremost by ensuring adversaries that their objectives will not be realized. A big bank vault does less to deter bank robbers than the presence of countermeasures (die packs, numbered bills, the FBI) that deny the robbers the fruits of their plunder, even when successful. Terrorism is a marginal business, not because airports and diplomats are too well protected or because guns or bombs are hard to come by, but because most people, even if very unhappy, do not believe that bombings, hijackings or assassinations will effect change. Incapable of achieving key objectives directly, terrorist organizations seek to mobilize fear and over-reaction.

The fact that terrorists may resort to cyberwar does not imply that cyberwar is an important threat to national security, any more than the fact that the poor or financially desperate are more likely to play the lottery implies that the odds of winning are inversely tied to one's income. Indeed, the rise of cyberterrorism may say more about the impotence of both agent and structure than about either in isolation. Cyber terrorism may be relatively ineffective, not unlike terrorism generally. Nevertheless, terrorists may adopt cyberwar even though internet attacks are unlikely to sway national policies or public opinion. The mere fact that terrorists adopt a method of attack does not mean that their actions represent an existential threat to national security, any more than do crime or corruption. Most societies treat the latter activities as separate from national security, not because they are unimportant or fail to harm people, but because they do not directly threaten the state. Countries may experience a growing number of cyber attacks in the future, but unless attackers have the ability to prosecute temporary advantages through physical force, it is unclear that cyber terrorism requires a particularly elaborate or concerted national security response.

Terrorism is a form of compellence. Lacking the ability to impose their will on others, terrorists rely on the prospect of harm to influence a target's behavior. Indeed, because their ability to harm

is quite limited, the terrorist relies on psychology (fear and uncertainty) to multiply the impact of relatively finite capabilities on opposing populations or governments. Cyberwar is arguably especially poorly suited to the task of fomenting terror. In particular, in addition to the problems in credibly threatening cyber attacks that have already been discussed, it is difficult to see how internet attacks will be able to instill the quality of fear needed to magnify the terrorist's actions. How terrifying is a cyber attack? No one will be happy when the power goes out or when one's bank account is locked down, However, attacks of this type evoke feelings if anger, frustration, even resignation, not terror. Terrorism relies on generating a particularly visceral emotion (the "terror" in terrorist), one that is not often effected through the actions of cyber warriors, at least (again) not directly. The old journalistic adage that "if it bleeds, it leads," implies the need for graphic trauma and lurid imagery. The very attributes that make cyberwar appealing in abstract — the sanitary nature of interaction, the lack of exposure to direct harm, striking from a remote location — all conspire to make cyber terrorism less than terrifying. White collar terrorists are unlikely to prove any more effective, perhaps less, at shaping hearts and minds than the traditional model.

This is even more the case with long-duration, low-intensity conflicts that are a key component of both non-western attempts at resistance and western efforts to protect the status quo international order. From the perspective of the insurgent, asymmetric warfare has never been about attacking to diminish an opponent's strengths, but is instead focused on maximizing one's own strengths by targeting the enemy's weaknesses (Mao 1961). Insurgency seeks out kinetic close physical combat where sophisticated technology is at its least effective (and decisive). Damaging the technology may draw an enemy into direct contact, but it might also cause that enemy to withdraw and reschedule operations. Mobility dominates every battlefield for this very reason. Internet attacks in the midst of close contact make little sense as it is here that the comparative advantage of cyberwar (distance and asymmetry) are least potent. The ability of internet-dependent armies to perform in superior ways on existing dimensions means that this is generally a process of leveling, not revolution.

5.3 Cyber Espionage

By far the most compelling scenario for the transformation of political conflict through the internet involves its use in espionage. As Wikileaks illustrates, it may become increasingly difficult for states to hide details of their capabilities and plans from individuals, groups and other nations.

Nations have always sought information about prospective opponents. Successful espionage creates significant advantages, but also challenges. For most of history, spying was physical. An agent had to enter enemy territory to obtain information about the capabilities or intentions of a foreign group or power. The products of espionage were equally tangible. Spies brought back documents, captives, tallies or other materials designed to inform their masters and demonstrate the veracity of their claims. This made spying risky. Espionage required an overt act that could itself tip nations into war. Evidence of spying could form the *causus belli* for an attack by a target against the perpetrator. Even if it did not lead directly to a contest, where agents were found, and what they were looking for, revealed sensitive information. For these reasons, counter-espionage is itself as much about spying as it is about preventing espionage. Of course, captured spies also fared poorly, as international norms offer none of the protections afforded to conventional combatants.

The internet makes it possible for the spy to telecommute. Information can be collected without leaving the territory of the sponsoring state, making it difficult to deter or capture cyber spies. A spy's affiliation can also be concealed, so that it is not clear to the target whether espionage indicates a prelude to war, threats from specific states, specific formal national objectives, or even whether espionage has actually occurred. At the same time, cyber spies face their own challenges and may actually be easier to detect than in conventional espionage, given the nature of computing.

One of the perennial challenges for political decision makers in dealing with any form of espionage is what to do with the information collected. It is tempting to act on covert knowledge, but often this will also tip off the target and lead to countermeasures. Even more fundamentally, the challenge to analysts is to interpret the significance of information, not something that the internet makes easier, particularly given the quantity of materials that are likely to be involved. Critical facts may even be obscured among masses of trivial details, protection not unlike the anonymity of mass humanity that shelters most of us, and is possible for information only in the internet age.

Conversely, it is entirely possible that the single most dramatic impact of the cyber world on political conflict will come in the form of transparency. Nations intent on maintaining national secrets may find that they can no longer sustain such secrecy. The phenomenon of classification that has led large chunks of government activity underground may find itself "outed," not by foreign terrorists or spies, but by groups that are devoted to the idea that airing national secrets makes it more difficult for nations to connive against one another, or to scheme against their own people.

There is some reason to believe that the decline of secrecy would also see a reduction in warfare, even if some nations are perhaps made worse off in terms of relative power. The conceit of sovereigns in past epochs was that secrets could be kept. To an astonishing degree this has never been true. Code breaking in both World Wars meant that German and Japanese operational plans were to a considerable degree an open book to Allied commanders. Similar results may have shadowed opponents during the Cold War. The problem of course was that espionage that unearthed enemy secrets also had to be kept secret, since there were advantages to knowing something that an enemy did not know that the opponent knew. Espionage did not reduce the prospect of war as much as it changed the distribution of power, since those in the know would be able to exploit relationships and win contests. Today, it may be increasingly difficult for nations to imagine that their secrets are safe, even if they are. In addition to "non-profit" espionage that releases information publicly, the ubiquity and effectiveness of "for profit" espionage in the internet age must make countries consider the likelihood that security is inherently porous. Nations must begin to assume that their secrets are not sacrosanct, making it more difficult to carry out the conspiracies so often associated with coercive politics. War will still be possible, but surprise in war will be increasingly difficult to achieve, in turn reducing at least part of the motivation behind the use of coercive military force.

6 Conclusion

In war, tactics must serve strategy and strategy must serve grand strategy. Students of cyberwar have yet to explain how the internet can host meaningful political conflict, precisely because it cannot serve the final arbiter function that has for millennia been the purview of physical violence. The tendency for pundits of cyberwar has been to focus on tactics and possibly strategy, showing

that harm is possible without explaining how the harm generated is likely to shape the product of political differences. In the absence of this logic of consequences, the internet becomes an adjunct domain to more traditional forms of warfare. Cyberwar is an evolving dimension of war and a source of concern, but in grand strategic terms, it remains a backwater. A failure to focus on grand strategy is an all-too-familiar byproduct of the war on terror, where the objective has been to harm and not be harmed, rather than to effect meaningful changes to the disposition of world affairs.

It would be absurd to infer that there is no role for the internet in twenty-first century contests. The internet will be affected by conflict, just as is the case with every other domain in which individuals, groups and societies interact. Indeed, the real message for soldiers and politicians is that cyberwar involves a broadening of the dimensions of warfare, rather than narrowing the future of conflict. In most cases the internet is not a viable free-standing venue for the fulfillment of national interests through interstate aggression. It would be surprising if a country intent on attacking another nation failed in the future to carry out preparatory or simultaneous attacks of the target's infrastructure and national defense capabilities thorough the internet. It would be even more surprising if an aggressor successfully substituted cyberwar for conventional, tangible forms of conflict. One of the greatest benefits a target could receive, in fact, would be for an attacker to be misguided enough to funnel its aggression into web-based war. This is the conceit of Nikolai Kuryanovich, former member of the Russian Duma, and other misguided shamans of cyberwar:

> In the very near future, many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers ... [22]

By itself cyberwar can achieve neither conquest nor, in most cases, coercion. Russian military planners obviously understood this in preparing to invade Georgia, not just with hackers, but with tanks. Indeed, the tanks appear to have done more to undermine Georgian security than anything accomplished by information soldiers. The threat of cyberwar cannot deter or compel particularly effectively either, except possibly in the short term, and only with the consequence that an attacker will have forfeited the potential to exploit a given set of vulnerabilities in the future. Cyber warfare

[22] Cited by Korns & Kastenberg (2008), who in turn reference Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks" *The Washington Post*, 16 October 2008,

will most often occur as an adjunct to conventional warfare, or as a stop-gap and largely symbolic effort to express dissatisfaction with a foreign opponent. It is best to discuss cyberwar in these contexts, not as an independent, or even alternative form of conflict, but as an extension of the logic already expressed in combined arms battle. Since in most cases cyberwar cannot achieve the objectives that have historically prompted nations to commit to tangible military violence, "cyberwar" is only really war in the context of terrestrial forms of interstate threats or force.

Even the most successful forms of cyberwar (such as cyber espionage) do not presage much of a transformation. Just as innovations in artillery and small arms made closed formations untenable, militaries, governments and societies will adapt. It would be ludicrous to suggest to modern infantry that their fires would be more concentrated if they stayed in formation while on the march. Contemporary field commanders have become comfortable with the idea that perimeters are partial or notional, that air-land battle (and naval warfare for a much longer time) necessarily involves not fronts, but mobility; not frontal assaults, but maneuver. Similar concepts will pervade discussions of cyberwar. Static security is insecurity. It does not follow, however, that being vulnerable means one will be attacked, or that there is much that can be done to prevent aggression if it is initiated. Security in a modern, integrated world — both in terrestrial and cyber — is a function more of the motives of opponents than of the ability to attack. Nations or groups that strike through the internet in minor ways may be ubiquitous. Those that threaten critical national security goals will be rare if for no other reason than that cyberwar is not really war in grand strategic terms. In this regard, the next Pearl Harbor is much more likely to occur at Pearl Harbor than in cyberspace.

References

Adams, James. 2001. "Virtual Defense." *Foreign Affairs* 80(3):98–112.

Adams, Karen Ruth. 2003. "Attack and Conquer?: International Anarchy and the Offense-Defense-Deterrence Balance." *International Security* 28(3):45–83.

Arendt, Hannah. 1970. *On Violence*. New York: Harcourt, Brace & Co.

Arquilla, John & David Ronfeldt. 1999. "The Advent of Netwar: Analytic Background." *Studies in Conflict and Terrorism* 22(3):193–206.

Biddle, Stephen. 1998. "Assessing Theories of Future Warfare." *Security Studies* 88(1):1–74.

Blainey, Geoffrey. 1973. *The Causes of War*. New York: Free Press.

Boulding, Kenneth. 1962. *Conflict and Defense*. New York: Harper & Row.

Buhaug, Halvard & Nils Petter Gleditsch. 2006. The Death of Distance?: The Globalization of Armed Conflict. In *Territoriality and Conflict in an Era of Globalization*, ed. Miles Kahler & Barbara Walter. Cambridge: Cambridge University Press.

Cerf, Vinton G. 2011. "Safety in Cyberspace." *Daedalus* 140(4):59–69.

Clark, David D. & Susan Landau. 2011. "Untangling Attribution." *Harvard National Security Journal* 2(2):25–40.

Clark, Wesley K. & Peter L. Levin. 2009. "Securing the Information Highway: How to Enhance the United States' Electronic Defenses." *Foreign Affairs* 88(6):2–10.

Clausewitz, Carl von. 1976[1832]. *On War*. Indexed ed. ed. Princeton, NJ: Princeton University Press.

Cohen, Eliot A. 1996. "A Revolution in Warfare." *Foreign Affairs* 75(2):37–54.

Courville, Shane P. 2007. "Air Force and the Cyberspace Mission: Defending the Air Force's Computer Network in the Future." Occasional Paper No. 63, Center for Strategy and Technology, Air War College.

Dunlap, Charles J. Jr. 2011. "Perspectives for Cyber Strategists on Law for Cyberwar." *Strategic Studies Quarterly* 5(1):81–99.

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

Fearon, James D. 1998. "The Offense-Defense Balance and War Since 1945." University of Chicago. Typescript.

Fuchida, Mitsuo. 1986. *Midway: The Battle That Doomed Japan*. New York: Ballantine.

Gartzke, Erik. 2006. Globalization, Economic Development, and Territorial Conflict. In *Territoriality and Conflict in an Era of Globalization*, ed. Miles Kahler & Barbara Walter. Cambridge: Cambridge University Press pp. 156–186.

Gilpin, Robert. 1981. *War and Change in World Politics*. New York: Cambridge University Press.

Glaser, Charles L. 1997. "The Security Dilemma Revisited." *World Politics* 50(1):171–201.

Glaser, Charles L. & Chiam Kaufmann. 1998. "What is the Offense-Defense Balance and Can We Measure It?" *International Security* 22(4):44–82.

Goldman, Emily O. & Leslie C. Eliason, eds. 2003. *Diffusion of Military Technology and Ideas*. Stanford, CA: Sanford University Press.

Gortzak, Yoav, Yoram Z. Haftel & Kevin Sweeney. 2005. "Offence-Defence Theory: An Empirical Assessment." *Journal of Conflict Resolution* 49(1):67–89.

Herz, John. 1950. "Idealist Internationalism and the Security Dilemma." *World Politics* 2(2):157–180.

Hollis, David M. 2011. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal* January(6):1–9.

Hopf, Ted. 1991. "Polarity, the Offense-Defense Balance, and War." *American Political Science Review* 85(2):475–494.

Hundley, Richard. 1999. *Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us About Transforming the U.S. Military.* Santa Monica, CA: Rand.

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

Knapp, Kenneth & William Boulton. 2006. "Cyber-Warfare Threatens Corporations: Expansion to Commercial Environments." *Information Systems Management Journal* .

Korns, Stephen W. & Joshua E. Kastenberg. 2008. "Georgia's Cyber Left Hook." *Parameters* 38(4):60–76.

Krepinevich, Andrew F. 1994. "Cavalry to Computer." *The National Interest* 37:30–42.

Krepinevich, Andrew F. 2002. The Military-Technical Revolution: A Preliminary Assessment. Technical report Center for Strategic and Budgetary Assessments Washington, DC: .

Levy, Jack S. 1984. "The Offense/Defense Balance of Military Technology: A Theoretical and Historical Analysis." *International Studies Quarterly* 28(2):219–238.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: Rand.

Lieber, Kier A. 2005. *War and the Engineers: The Primacy of Politics over Technology.* Cornell University Press.

Lindsay, Jon. 2012. "Stuxnet and the Ambiguous Nature of Cyberwar." Paper presented at the Annual Meetings of the International Studies Association, San Diego, CA. April 1-4.

Lynn III, William J. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89(5):97–108.

Lynn-Jones, Sean. 1995. "Offense-Defense Theory and Its Critics." *Security Studies* 4(4):660–691.

Lynn, William J. 2011. "The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack." *Foreign Affairs* .

Mao, Zedong. 1961. *On Guerrilla Warfare.* New York: Praeger.

Maurer, Tim. 2011. "The Case for Cyberwarfare." *Foreign Policy* .

McNeill, William H. 1984. *The Pursuit of Power: Technology, Armed Force, and Society Since A.D. 1000.* Chicago: University of Chicago Press.

Mearsheimer, John J. 1983. *Conventional Deterrence.* Ithaca, NY: Cornell University Press.

Morton, Louis. 2000. Japan's Decision for War. In *Command Decisions*, ed. Kent Roberts Greenfield. Center of Military History, Department of the Army Washington, D.C.: U.S. GPO chapter 4, pp. 99–124.

Nalebuff, Barry. 1991. "Rational Deterrence in an Imperfect World." *World Politics* 43(3):313–335.

O'Hanlon, Michael. 2000. "Why China Cannot Conquer Taiwan." *International Security* 25(2):51–86.

Parshall, Jonathan & Anthony Tully. 2007. *Shattered Sword: The Untold Story of the Battle of Midway.* Herndon, VA: Potomac.

Powell, Robert. 1990. *Nuclear Deterrence Theory: The Search for Credibility.* Cambridge: Cambridge University Press.

Prange, Gordon W. 1981. *At Dawn We Slept: The Untold Story of Pearl Harbor.* New York: McGraw-Hill.

Prange, Gordon W. 1983. *Miracle at Midway.* New York: Penguin.

Quester, George H. 1977. *Offense and Defense in the International System.* New York: John Wiley & Sons.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *The Journal of Strategic Studies* 35(1):5–32.

Schmitt, Michael N. 2010. Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, ed. Committee on Deterring Cyberattacks. National Research Council Washington, D.C.: National Academies Press pp. 151–178.

Schweller, Randall L. 1996. "Neorealism's Status-Quo Bias: What Security Dilemma?" *Security Studies* 5(3):90–121.

Sheldon, John B. 2011. "Deciphering Cyberpower: Strategic Purpose in Peace and War." *Strategic Studies Quarterly* 5(2):95–112.

Shimshoni, Jonathan. 1991. "Technology, Military Advantage, and World War I: A Case for Military Entrepreneurship." *International Security* 15(3):187–215.

Slantchev, Branislav. 2010. "Feigning Weakness." *International Organization* 64(3):357–388.

Snyder, Jack L. 1984. *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914.* Ithaca, NY: Cornell University Press.

Symonds, Craig L. 2011. *The Battle of Midway.* New York: Oxford University Press.

Toffler, Alvin & Heidi Toffler. 1993. *War and Anti-War: Survival at the Dawn of the 21st Century.* Boston: Little, Brown, and Co.

Valeri, Lorenzo & Michael Knights. 2000. "Affecting Trust: Terrorism, Internet and Offensive Information Warfare." *Terrorism and Political Violence* 12(1):15–36.

van Creveld, Martin. 1989. *Technology and War: From 2000B.C. to the Present.* New York: Free Press.

Van Evera, Stephen. 1998. "Offense, Defense, and the Causes of War." *International Security* 22(4):5–43.

Vickers, Michael G. & Robert C. Martinage. 2004. The Revolution in War. Technical report Center for Strategic and Budgetary Assessments Washington, DC: .

Walt, Stephen M. 2010. "Is the Cyber Threat Overblown?" *Foreign Affairs* .

Waltz, Kenneth N. 1990. "Nuclear Myths and Political Realities." *American Political Science Review* 84(3):731–745.