The US Army War College Quarterly: Parameters

Volume 41
Number 3 *Parameters Autumn 2011*

Article 12

8-1-2011

Cyberweapons: Leveling the International Playing Field

Ross M. Rustici

Cyberweapons: Leveling the International Playing Field

Ross M. Rustici

One of the largest security concerns facing the United States today is how to mitigate its vulnerability to cyberweapons. Over the past twenty years, cyberthreats have evolved from solitary hackers motivated by monetary gain and prestige to organized crime and state actors. The sophistication and capabilities of these threats grows in direct proportion to the level of connectivity in society. Despite this steady development of cyberthreats, relatively little attention is given to discerning how these threats will impact warfighting and the international system. Most of the current literature on cyberwarfare considers it, at best, a force multiplier. Many scholars disregard its effects as a standalone attack vector, citing various reasons from US responses to Pearl Harbor and 9/11 to the inability of strategic bombing in World War II to subdue the civilian populations in England and Germany, absent combined military operations. These perspectives are correct in arguing that offensive cyberoperations without traditional, conventional power will be largely futile. This analytical approach, however, presumes that cyberweapons will be used in an offensive, first-strike manner. The long-range strike capabilities of cyberwar have the potential to be extremely effective when employed as an anticoercion weapon. In essence, a strong cyber capability is a deterrent force that will largely mitigate outside interference in domestic and regional affairs.

Because there are no confirmed cases of a large-scale, state-sanctioned cyberattack, analysts are currently forced to explore different weapon systems and theories to help both the fighter and the politician understand how cyberweapons can be utilized and what vulnerabilities this new class of weapon creates. Given the unique characteristics of cyberspace and cyberweapons, no existing technology or theory will provide an adequate understanding. Nevertheless, by borrowing tenets from both strategic airpower theory and early debates on nuclear weapons doctrine and deterrence, the approximate capabilities of cyberweapons become far less opaque.

Mr. Ross Rustici is a contract Research Analyst who has worked with the National Defense University's Institute for National Security Studies. His expertise lies in US-Chinese strategic relations and the People's Liberation Army including PLA Navy operations, force sizing, and defense transparency.

The concept of strategic airpower has developed over the past century into one of the main tenets of modern war.[1] Strategists understand its limitations in winning a war of existential proportions but also found it exceedingly useful in short duration conflicts between two unequal parties. The air superiority required for a strategic air campaign costs trillions of dollars and requires an extensive network of overseas bases for airfields and ports that can accommodate carrier battle groups. This level of investment is beyond the capacity of most states. As a result, cyberweapons have the potential to become an equalizing force because they require a fraction of the investment but are able to execute most of the same missions.

Additionally, early nuclear theory wrestled with many of the same problems that we now face in attempting to understand cyberweapons. While the United States and Soviet Union eventually came to the same conclusion about the true utility of nuclear weapons in war, it took two decades to do so. While cyberweapons may turn out to be awe inspiring enough to create a new form of mutually assured destruction (MAD)[2], it is far more likely that early thinking regarding demonstration shots and defense on the cheap dovetailing into massive retaliation will be more insightful.

Just as the industrial revolution brought about a fundamental change in warfare, the information age is ushering in a new, low-cost option for strategic defense. Cyberwarfare capabilities can now accomplish most of the strategic tasks that once required air supremacy. According to US analysts, everything from health care to the power grid is a viable cyber target.[3] A cursory look at the targets of recent US air campaigns illustrates how much civilian infrastructure is targeted in a strategic bombing campaign. In today's interconnected world, both civilian infrastructure and military installations are increasingly vulnerable to cyber disruption.[4] As a result, the future of warfare and the limits on international coercion have the potential to fundamentally shift.

This article examines how cyberweapons pose new risks to networked societies, explores the specific impact they might have on the United States, and the implications of these new cyber capabilities. The article concludes with a brief discussion of the possible limitations and problems with using cyberweapons in a deterrent fashion. This article is not meant to be definitive or advance specific policy options; rather, it is meant to be a first step toward thinking about the application of cyberweapons in the defense policy of others and its ramifications for United States freedom of action.

Emerging Cyberthreats

To understand the true possibilities of these weapons, one must first delineate the distinction between Computer Network Exploitation (CNE) and Computer Network Attack (CNA). CNA is the act of disruption, denial, degradation, or destruction (4Ds) of computer networks, the information contained within the network, or systems controlled by it. CNE is essentially an intelligence gathering activity. While an actor attempting CNE occasionally makes a mistake that results in one of the 4Ds, instances of deliberate CNA

are exceedingly rare. While the United States and the rest of the world suffer CNE activity on the scale of millions of attempts a day, to date there have only been a handful of overt cases of significant CNA. While there are hacker wars that rage almost on a daily basis, the defacing of websites hardly qualifies as CNA on the level of state sanctioned violence. Estonia, Georgia, and Iran provide the most well-publicized instances of significant CNA, and perhaps the only suspected instances of state sponsored CNA. Due to the dearth of actual case studies, those writing on the subject of CNA are forced to look at what is technically feasible and postulate from that. While the number of reported cases of CNE is exponentially rising as the targets are increasingly sensitive and the level of exploitation is unparalleled, global CNA capabilities are largely unknown and untested.

Extrapolating from CNE capabilities and what little documentation there is on CNA and cyberweapons, we know advanced actors are able to power down electric grids, paralyze rail systems, distort stock markets, damage water purification and waste treatment plants, open dams, and shut down oil refineries.[5] In a society as networked as the United States or Europe, most, if not all, of the critical civilian infrastructure is vulnerable to cyberattacks. Given the speed and precision with which a cyberattack can be carried out, these weapons can be used for anything from a warning shot to signal an adversary in a crisis to a catastrophic strike that could cost a state trillions of dollars and an untold number of lives. This wide range of applications makes cyberweapons unique, and the fact that a cyber arsenal is also exceedingly cheap means that the available destructive capacity for poor or weak states is unprecedented. The ability to strike quickly, without warning, and on such a large scale makes them uniquely terrifying. A well-executed cyber campaign coupled with careful public relations has the potential to traumatize a society in ways not seen since Nagasaki.[6] While cyberweapons do not create the same spectacular visual that a nuclear or even conventional missile does, the means by which they are delivered make them an inherent tool of psychological warfare. Unlike conventional or even nuclear weapons, there is no advance warning of an incoming cyberattack. The inability of a society to harden itself to an expected, incoming attack furthers the effectiveness of cyberweapons. Not knowing what the next attack is going to be or when it will happen has a profound effect on the victim and makes cyberweapons unique amongst all possible coercive systems.

That said, a cyber "Pearl Harbor" makes little sense for the majority of the world. Despite these glaring vulnerabilities, without conventional capabilities to exploit a confused and disorganized population, cyberattacks will most likely cause civilian support for the government rather than capitulation. The Estonia and Georgia events illustrate this phenomenon. In Estonia, the Russian hacker community paralyzed media outlets, certain bank functions, and government websites for several days in retaliation for the Estonian government's decision to move a statue honoring the Soviet military out of Tallinn. Because there was no corresponding military intervention, however, capitalizing on the effects of the cyber campaign, the effects were largely financial and short term.[7]

The state did not return the statue to its original place, and as a result of the attacks Estonia presumably became more secure because of enhanced engagement and leadership with NATO. The Georgian war, on the other hand, relates a very different story. The cyberattacks were coordinated with a Russian military operation and acted as a force multiplier. While the attacks themselves did not have any lasting ramifications, the show of force arguably shifted Georgia back into Russia's sphere of influence. In both cases, Russian hackers showed remarkable restraint in selecting their targets. Critical infrastructure was not targeted in either case and long-term damage was negligible,[8] but despite this relatively low-level targeting, the psychological and economic impacts were large.

Given how few incidents of cyberwar there are, analysts are forced to speculate about the uses and effects of larger, more targeted attacks. How would the American population react to the hardships of a strategic cyberattack as a result of US intervention abroad? While there is no reliable data about how America would respond to severe, conflict-induced hardship, some tentative conclusions can be drawn from the way in which public opinion has shaped the use of force over the past two decades. Findings show that the American public's casualty aversion is directly related to two perceptions. First, they need to believe that the stakes are important. Second, they need to understand that the prospect for success is high. If either of these conditions is not met, then tolerance for casualties and support for military action rapidly wanes.[9] This trend was exemplified in the Kosovo campaign. The Clinton administration insisted on not committing ground forces largely because of political backlash it experienced in the wake of the conflict in Somalia. The air-only campaign, while effective, demonstrates the extremes that the United States is willing to go to prevent casualties.

This low threshold for casualties abroad[10] should translate into an even more risk-adverse position when considering threats to the civilian population in the United States. Indeed, anecdotal evidence shows that, when faced with a catastrophe at home, democracies tend to withdraw support for nonvital missions abroad. A recent illustration is the Spanish withdrawal from Afghanistan. Many attribute the terrorist attacks on the Spanish subway as being the catalyst for the Spanish Socialist Workers' Party to gain control of the government, resulting in the withdrawal of Spanish forces from Afghanistan. Polling data in Spain showed that the general population never regarded the United States' War on Terror as advancing Spanish national security.[11] Additionally, the Madrid bombings illustrated that, despite three years of war, the likelihood of any form of demonstrable success was still low. This case illustrates that civilian populations are more risk adverse when the costs are more likely to affect them directly.[12]

The justification for Operation Enduring Freedom further lends support to this concept of protecting the homeland against any risk. The main argument for war with Iraq was Saddam's weapons of mass destruction (WMD) program. The logic was that the United States and its coalition forces must invade to disarm Iraq and preempt Saddam from possibly attacking the United

States or its allies. This official position was supported by public opinion polls; 70+ percent of Americans thought the war was justified as late as May 2003.[13] Historically, the American population has supported interventionist policies that were rationalized as protecting the American way of life.

The discussion above is indicative of what foreign policy constraints America will face in the 21st century. Cyber capabilities can be leveraged to cause widespread economic loss and even casualties. The Madrid train bombings that so drastically altered the course of Spain's foreign policy could largely be replicated through a cyberattack. The potential for an advanced cyber foe to wreak chaos on the American homeland is unparalleled. Not since the War of 1812 has a potential adversary had the capability to strike the continental United States without representing an existential threat. Cyber capabilities are cheap, effective, and can be utilized from anywhere in the world, at any time. Cyberwarfare will likely represent a new force paradigm that reduces the instances of interstate conflict and greatly reduces armed humanitarian intervention due to increased transactional costs.

Hegemonic Security

The American global defense posture since the end of World War II has been primarily one of offshore balancer. In the most simplistic of views, the United States spent the Cold War and subsequent decades trying to preserve regional balances of power and prevent any coalition from gaining a disproportionate amount of power. This balancing has ranged from active conflict in Korea, Vietnam, and Iraq to support activities in the Middle East, Africa, and Southeast Asia. Not since World War II has America fought in a conflict or supported an interventionist foreign policy where its adversaries had the military capability to severely harm the United States. Indeed, it has not been since the Spanish-American War that the United States has fought a military with a global reach and military bases within striking distance of the continental United States. Not since the war of 1812 has the continental United States experienced an invading force. This amazing insulation from conflict is eroding quickly as technology progresses. While the United States, due largely to geography, has had the ability to act internationally with impunity, this is no longer the case. Cyber capabilities allow, for the first time in history, small states with minimal defense budgets to inflict serious harm on a vastly stronger foe at extreme ranges.

To be clear, cyberweapons merely increase the cost of conflict for adversaries; these weapons are unlikely to dissuade national security policy when core national interests are at stake. With the exception of the United States and the United Kingdom, there are no countries with a demonstrated global power projection capability able to take advantage of the situation created by an effective cyberattack beyond their immediate borders. Cyberattacks on critical infrastructure thus become primarily a defensive weapon. These capabilities have the potential to provide substantial regime security at a fraction of the cost of a nuclear weapons program. While the deterrent value may be less

than nuclear weapons attached to intercontinental ballistic missiles (ICBMs), a cyberattack has the potential to inflict enough damage to prevent interventionist foreign policy. The transaction cost for the United States to act as an offshore balancer or a global police force will increase dramatically. This is likely to erode the American public's tolerance to the ramifications of intervention in anything but the most extreme circumstances.

Implications

The importance of the conventional asymmetric balance of forces between the United States and the rest of the world is one of the major determining factors of this analysis and cannot be stressed enough. As discussed in previous sections, cyber capabilities in large part mimic the repercussions of America's strategic bombing campaigns. Cyberweapons targeting critical infrastructure will have the ability to reciprocate the result of traditional air strikes in a way that the United States has never experienced before. It is in this way that these weapons greatly constrain America's use of force abroad.

There are three possible implications of the advent of capable cyberweapons. The first is a curtailing of interstate coercion. As a consequence of the first, the second is a derailment of the human security initiative as argued by proponents of Responsibility to Protect. Finally, cyberweapons present the possibility of altering conventional force structures in a fundamental way.

The most likely impact of cyberweapons is to severely curtail the use of sanctioned interstate violence. Just like large and capable conventional forces, cyberweapons present a strong deterrent for a potential attacker. Cyberweapons are a cheap way to build a global strike capability against networked states. While the United States may be the only state outside of the Middle East capable of putting bombs over Baghdad, soon any country with a network connection may be able to paralyze a nation's capital. As a result of this capability, interventionist foreign policies will become exceedingly costly, not just in the material and lives of the armed services, but on the home front as well. The new dangers that this fifth domain of warfare creates mean that only the most fundamental national security issues will be worth risking the potential retaliatory strikes.

This leads to a serious reconsideration of the concepts of global security and the human security initiative, all while causing a retrenchment of the classical Westphalian state-centric system. If Iraq or Yugoslavia had advanced cyber capabilities, the likelihood of air strikes against institutions of the state would have been drastically reduced. The cost of intervention increases with a target state's ability to successfully launch a strategic cyberattack. How many states are willing to prevent humanitarian crises if it means a five to seven percent reduction of their own gross domestic product (GDP),[14] on top of the costs required to execute the military action? Furthermore, unlike hypothetical disarming first strikes with conventional or nuclear weapons, the flexible and landless nature of cyberspace makes it impossible to have any measure of confidence regarding the effectiveness of the strike. Unlike in the other four

domains, it is impossible to see a neutralized cyberweapon in cyberspace. Neither offensive nor defensive measures can alleviate these higher transactional costs with any degree of certainty.

Finally, cyberweapons have the ability to greatly reduce the need for an expansive global air force. This is especially true for rising powers, or those facing the need to modernize their fleet. While air superiority is still necessary for invasion and—at least in the near future—counterforce operations, its usefulness as a strategic weapon is rapidly declining. There are multiple comparative advantages of cyberweapons over air strikes. The first and most compelling is cost. Cyberweapons cost a fraction of the cost of missiles and do not require complicated and expensive system platforms to deliver them. Anyone with a laptop can launch a cyberattack, whereas stealth bombers cost billions. In addition to cost, the temporary nature of cyberattacks makes them far more appealing when considering postwar reconstruction. If a combatant can disable a power grid for four days, and then with a flip of the switch turn all the lights back on, it is immensely cheaper, and makes reconstruction efforts easier, than bombing a power plant and rebuilding it. Furthermore, while there may be ripple effects within the networks themselves, cyberattacks eliminate almost all chance of collateral damage.

These implications mean that the future of warfare and the limits on international coercion are likely to fundamentally shift. Cyber deterrence is capable of reducing the incidents of violence in the international system; however, it is also likely to make the world a safer place for corrupt and abusive regimes. Cyberweapons, and their deterrent value, do not rival that of nuclear weapons, but they do have the potential to be a greater deterrent force than conventional systems. Their deterrent value may not matter between adversaries fighting over core national interest, but cyber capabilities will matter a great deal when peripheral interests are at stake. They have the potential to increase the transactional cost of war to such an extent that the United States, or any advanced society, will be far less willing to use force internationally based on ideals or a perception of a marginal regional balance of power.

Failures of Deterrence

There are, however, glaring issues regarding deterrence in cyberspace. Unlike nuclear weapons or any conventional capability, it is almost impossible to demonstrate cyberpower. Furthermore, it is very easy to develop this capacity with an exceedingly small footprint. The technical nature of cyberweapons requires a preexisting problem in a particular piece of software or the ability to assume the identity of a trusted user to carry out an attack. In cyberspace, the use of any attack results in a near perfect defense within days or at most months against the reuse of that specific exploit. Unlike conventional weapon systems, cyberweapons rely on man-made vulnerabilities. They do not exert a physical destructive force; instead they operate much like water running through a poorly constructed dam. Water can only pass through it if cracks are present. Similarly, cyberweapons can only penetrate network defenses if there

are exploitable flaws in those defenses. A distributed denial of service attack (DDoS), such as the ones that hit Estonia and Georgia, is comparable to water spilling over the top of a levy. If those attacked stem the flood of internet activity, the DDoS attack will be stymied. Once a DDoS is executed, it is possible to prevent the machines used to execute the attack from calling out to the Internet again. This means that any attack, even for demonstration purposes, ends up being an irreplicable weapon system. As such, cyber deterrence is forced to rely almost entirely on a perverse form of blind man's bluff. Not only would the United States not know if a potential adversary has cyber capabilities to inflict serious harm on critical infrastructure, but it also does not know at what point that adversary would use them. As these weapons proliferate, it will be increasingly dangerous for America to actively shape the international arena through coercive means. Yet policymakers in the United States will have little indication of how large a threat countries pose.

There are, however, some crude indicators of how advanced an attack might be. For instance, intelligence operations and low-level hacks are often used to learn about the interaction of networks. Mapping the targeted power grid and other critical infrastructure is exceedingly useful, but not necessary for a successful cyberstrike. Stuxnet proved that as long as a state has the ability to test a cyberweapon on a system similar in composition to its target it can still be very successful. Thus, it would be possible to build a cyberweapon with the only trace being international procurements of commercial control systems. Because most of the technology needed to develop sophisticated cyberweapons is commercially available and completely unregulated, traditional technology and arm control regimes are impossible to create and verify. This makes it nearly impossible to track the development of cyberweapons. Indeed the only way we can currently estimate the cyber capabilities of another actor is by measuring the frequency and sophistication of attacks emanating from a state.[15]

The relative ease with which a state, or even individuals, can develop these capacities is enough to give serious security thinkers pause.[16] Couple this with a general inability to accurately assess these capabilities and it is almost guaranteed that the United States, or any other large conventional military power, will misjudge its opponent and pay dearly for the mistake. Once this particular Rubicon is crossed, the world will not be able to turn back.

Conclusion

Previously articulated strategic military doctrines have the potential to provide us with a concrete development path for the utilization of cyberweapons. Given the similarity between airpower and cyberpower regarding targeting, it is easy to present the parallels and accept strategic airpower doctrine as the guiding principles in the early stages of cyberweapons development. Likewise, early debates regarding nuclear weapons and deterrence are applicable to the way in which people currently view cyberwarfare. Despite these linkages, the uniqueness of cyberweapons makes the application of existing theories a dangerous proposition that hinders our understanding of how

these weapons can and will be utilized. Cyberweapons have the unique ability to change international relations in ways never seen before. Cyber deterrence is truly defense on the cheap. A defense budget measured in hundreds of millions can effectively deter one measured in hundreds of billions. Furthermore, there is currently no international norm against the acquisition or deployment of these weapons. Finally, the distinctive psychological impact of cyberweapons cannot be underestimated. The inability of a society to fortify itself against an incoming attack greatly increases the toll that attack takes on the society. The confluence of these factors creates a situation where deterrent weapons are affordable and acquirable within the existing international system. This greatly increases the likelihood of constrained international action by powerful countries. Without effective cyber defense, offensive military power will be a less credible way to induce change. Networked societies will be far more cautious in advocating for humanitarian intervention, regime change, no-fly zones, and other nonessential security operations. When core interests are at stake, the potential physical and psychological damage is unlikely to be a large enough deterrent to prevent conflict. The high cost associated with that conflict is likely to make the actors involved exercise extreme caution and exhaust all avenues before conflict becomes a viable option.

If cyberweapons develop along these lines, the United States and other advanced, networked states face fundamental tradeoffs. Unlike nuclear weapons and the Cold War, no country can hope to build sufficient offensive power to dissuade the use of cyberweapons in retaliatory strikes. The very nature of cyber deterrence as described above is being driven by overwhelming conventional inferiority. Building further offensive prowess will only increase the likelihood of a small state resorting to disproportionate strikes sooner in a crisis, rather than being dissuaded. Furthermore, should a conflict erupt, any hope of mutual cyber deterrence breaks down. Unlike the nuclear threshold, the same vulnerabilities that allow cyber deterrence to tentatively work are high priority targets of air campaigns. Once an air strike incapacitates or otherwise harms critical infrastructure, there is nothing to prevent the attacked state from unleashing a cyber retaliation.

This leaves the United States and other advanced states with stark policy considerations; while not mutually exclusive, none of these options constitute a satisfactory solution to this problem. First, network-reliant states, in an attempt to create adequate defenses, can resort to strict network controls, monitoring all transferred data on a scale even greater than we currently see in the most repressed countries. Second, states could adopt a counterforce-only strategy. This would allow states to still take military action but limit their actions only to attacks on dedicated military hardware. While this would greatly limit a state's ability to wage war effectively, it would also help to create a taboo against any strikes on civilian infrastructure. This would help to mitigate networked states's vulnerability to cyberweapons and still allow them a degree of freedom to intervene internationally. The final option is simply to accept that the transactional cost of war has increased. None of these options are appealing

for a country wishing to maximize its flexibility in dealing with world events. Nevertheless, cyberweapons—if developed along the lines described above—will force states to broadly pursue, in varying degrees, all the options listed.

While it is too early to determine if any of these potential trends will come to reality, these issues deserve further analysis. The value of cyberweapons will, in all likelihood, fall somewhere in the grey area between a strategic nuclear strike and the advanced conventional forces optimized by the United States Air Force. While security theorists are often quick to pronounce new weapon systems as being transformative, in the case of cyberweapons the potential is truly there. Cyberweapons have the latent ability to usher in a new international order founded upon a byte-based MAD. However, as with every system before it, cyberweapons's ghastly effects on the world order will only be understood once they are employed and the world can see the effects firsthand. The next decade will be critical to the development of cyberweapons and how they will be employed by various states. Until we as a nation and a member of the global community truly understand the full application of cyberweapons in the international system, we cannot hope to formulate effective policy.

Notes

1. For a discussion of the evolution of strategic air power, see Mark J. Conversino, "The Changed Nature of Strategic Air Attack" Parameters 27, no. 4 (Winter 1997-98): 28-41.

2. In recent Congressional testimony, General Alexander has already stated that some sort of deterrence based on mutual vulnerability may exist among the more powerful nations.

3. For further discussion of targets already affected, see McAfee's report "In the Crossfire: Critical Infrastructure in the Age of Cyberwar" http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf (accessed April 17, 2011); William J. Lynn III, "Defending a New Domain" *Foreign Affairs*, 89:5; Lawrence Gershwin's Statement for the Record to the Joint Economic Committee on Cyber Threat Trends and US Network Security, 21 June 2001 http://www.dni.gov/nic/testimony_cyberthreat.html (accessed April 17, 2011).

4. Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010). Additionally, Director Panetta, in Congressional testimony before the House Intelligence Committee, recently highlighted that cyberattacks have the potential to paralyze the country.

5. This list is merely illustrative. Anything that is controlled at least in part by a computer is vulnerable to cyberweapons. Systems with access to the Internet are easier targets; however, the Stuxnet case illustrates that even air-gaped systems are vulnerable.

6. A hypothetical cyber campaign could unfold in the following manner: 1) mid-air collisions of civilian airlines coupled with derailments of AMTRAC and commuter or subway trains; 2) cell phone blackouts; 3) gas line ruptures, oil refinery shut downs, and the breaching of dams though utilizing the emergency release valves; 4) the state launching the cyberattack announcing responsibility; 5) cutting the national power grid. The resulting loss of life, economic losses, and sense of victimization has the potential to fundamentally destroy a state's will to continue offensive action.

7. William C. Ashmore, "Impact of Alleged Russian Cyber Attacks," *Baltic Security & Defence Review*, Volume 11, 2009.

8. In the case of Estonia, the main targets were government websites, major media outlets, and banks. The primary mode of attack was DDoS. In the case of Georgia, the main targets were also government websites and media outlets. Critical infrastructure such as the SCADA systems

controlling the Baku–Tbilisi–Ceyhan pipeline was unaffected. It appears the primary purpose of the cyberattacks was psychological warfare.

9. Eric V. Larson and Bogdan Savych. "American Public Support for U.S. Military Operations from Mogadishu to Baghdad" (Santa Monica, CA: RAND Corporation, 2005), 219.

10. The connection between casualties abroad and hardship at home is accentuated by the transition to an all-volunteer military. The lack of a conscript military transfers the burden of military service from society at large to minority segments. The fact that the greater polity still reacts as negatively to the death of US servicemembers despite being largely insulated from the costs demonstrates America's severe casualty aversion.

11. Gallop International Post Iraq War Poll Europe conducted in 2003—63 percent of respondents judged that military actions in Iraq and Afghanistan made the world a more dangerous place.

12. The action-reaction paradigm cannot be stressed enough when considering the Spanish case. Unlike 9/11, the Spanish population viewed the Madrid bombings as a direct result of their role in Afghanistan, thus causing the cessation of combat activities. The fact that the population linked their foreign policy to causing a catastrophe at home demonstrates general risk aversion. In the case of 9/11, Americans viewed themselves as victims of an unprovoked attack. This distinction in the cause and effect relationship is fundamental to understanding how a democracy will react to a large-scale cyberattack.

13. Dana Milbank and Jim VandeHei "No Political Fallout for Bus on Weapons," *The Washington Post,* May 17, 2003, http://www.washingtonpost.com/ac2/wp-dyn/A1155-2003May16 (accessed April 2, 2011).

14. Estimates based upon Scott Borg's presentation at the 19th annual USENIX Security Symposium entitled "How Cyber Attacks Will Be Used in International Conflicts."

15. This method is crude and often very unreliable given that most forensics can, at best, trace an attack back to a computer. This provides no information about the person using that computer. Just because an attack originated in a country does not reliably prove that a government was involved. Thus, we may vastly over- or underestimate a state's actual capability based on this very crude metric.

16. A cursory Internet search turns up countless news stories detailing attacks by rogue regimes exhibiting advanced capabilities, teenage hackers using relatively unsophisticated methods to gain control of critical infrastructure, and cyber extortion schemes affecting public power grids and oil refineries. A recent security test of a water purification plant's IT security showed fatal and easily exploited vulnerabilities. Attacks on critical infrastructure and government systems are happening with alarming frequency. The ability of poorly financed hackers pursuing their trade for intellectual or monetary reasons is perhaps the only reason we have not seen a major cyber incident. Based on these incidents, the extrapolation to what a well-organized and financed state is capable of is not a great leap.