Cyberwar as a Confidence Game

Martin C. Libicki

Is CYBERWAR the twenty-first-century version of nuclear war? Readers of the *Economist*, whose 3–9 July 2010 cover portrayed a digitized nuclear explosion in the midst of a city, could be forgiven for thinking so. The takeaway was obvious: cyber weapons are now the latest class of strategic weapons, they can do enormous damage to societies, and the first recourse against this threat should be some sort of arms control. Otherwise, the bad old days of strategic confrontation would be back, but this time with scores of countries and no small number of nonstate actors, transnational criminal organizations, and a few overindulged high school students having the requisite capability to build weaponry that can bring life as we know it to a prompt halt.

Such a scenario could happen, but to see cyber weapons as primarily strategic in the same way as nuclear weapons is quite misleading. A more plausible strategic rationale for the United States' developing cyber weapons is to make *other* states think twice about going down the road toward network-centric warfare as the United States is doing, thereby extending its lead in this area. Cyber weapons do so by making other states—already lacking confidence in their ability to handle high technology—doubt that their systems will work correctly when called on, particularly if used against the United States or its friends.

This logic is explained in three parts, starting with a brief description of cyber attacks and their effects. Next, the case is made against assuming that cyberwar can be used for its strategic impact, followed by the case for thinking that the *threat* of cyberwar might possibly shape the investment decisions of other states to the advantage of the United States.

Martin C. Libicki, PhD, is a senior management scientist at RAND Corporation, focusing on the impacts of information technology on domestic and national security. He has published *Conquest in Cyberspace: National Security and Information Warfare and Information Technology Standards: Quest for the Common Byte*, as well as numerous monographs. Prior employment includes the National Defense University, the Navy Staff, and the GAO's Energy and Minerals Division. He holds a master's degree and PhD from the University of California–Berkeley.

Cyberwar: A Précis

There are critical differences between cyberwar and physical war.[1] These differences are so great that tenets about the use of physical force are imperfect guides to cyberspace. To summarize, cyberwar is the systematic use of information (bytes, messages, etc.) to attack information systems and typically, by so doing, the information that such a system holds.

Cyber attacks are enabled by (1) the exposure of target systems to the rest of the world, coupled with (2) flaws in such systems which are then exploited. Systems vary greatly in their susceptibility to cyber attacks, and such susceptibilities may also vary over time, especially before and after an attack. System owners are typically unaware of the exact nature of serious flaws of their own systems; otherwise they would not be flaws very long. They may not realize how exposed they are to the rest of the world. Yet, cyber attacks are self-depleting.[2] Once a vulnerability has been detected, often by dint of its being exploited and deemed consequential, efforts usually follow to eliminate the vulnerability or reduce a system's susceptibility to further such attacks.

The direct effects of cyber attacks are almost always temporary. Rarely is anything broken (the Stuxnet worm perhaps a prominent exception). At the risk of a little oversimplification, because a cyber attack consists of feeding systems the wrong instructions, replacing such instructions in favor of the original correct instructions returns control to the owner.[3]

The prerequisites of a cyber attack are clever hackers, cheap computer hardware, a network connection, intelligence on the workings and role of the target system, specific knowledge of the target's vulnerabilities, and the tools to exploit such vulnerabilities. Cheap computer hardware possibly aside, none of these can be destroyed in a cyber attack. Furthermore, none are the exclusive province of states, although states have distinct advantages in acquiring these prerequisites.

Cyber attacks are very difficult to attribute. Determining which machine or network the originating attack came from is challenging enough, but even knowing that much does not prove that its owner was responsible, because there are many ways for a hacker to originate an attack from someone else's box. Even finding the specific hacker does not necessarily prove that a state was responsible for his or her actions.

It is hard to predict the effects of cyber attacks, even those directed against well-scoped targets. Systems change constantly; processes that depend on affected systems' collateral damage are not readily apparent

and cannot necessarily be inferred from their physical properties. The ultimate cost of, say, a disruption is proportional to the time required to detect, characterize, and reverse its damage—all of which can vary greatly. Even after a cyber attack, it may not be clear what exactly happened; a data/process corruption attack, for instance, loses much of its force if the target knows exactly what was corrupted. What an attacker believes it did (much less its purpose) may differ from what happened, which in turn may differ from what the target perceived to happen.

Cyberwar does not sit on top of the escalation ladder, or even very close to the top. Thus, it is not necessarily the last word between states.

Cyber Warfare as Operational Warfare

Cyber attacks have a potentially important role to play against unprepared and unlucky adversaries that have enough sophistication to acquire and grow dependent upon information systems but not enough to defend them against a clever and persistent attack. Nevertheless, as suggested above, the effect of such an attack tends to be limited in time and scope. The fact that cyber attacks rarely break things means that the effects on systems are temporary. In that respect cyber warfare is, like electronic warfare, a facilitator of kinetic attacks. Indeed, both have been mooted against the same targets (e.g., SAMs). But electronic warfare has a serious advantage as a weapon that cyber weapons lack. It takes place outdoors, so to speak, where both sides contend for access to the same spectrum; factors such as the ability to generate a powerful signal can overwhelm a perfectly executed but weaker signal from the other side. To a first-order approximation, the environment is a given. Cyber warfare, however, takes place indoors, specifically in the systems of the target. Its ability to succeed has everything to do with the characteristics of the system being attacked. There is no forced entry, and a perfectly executed system is impenetrable; whereas perfection is not given to mortals, a completely disconnected, hence practically invulnerable, system is plausible.

Both electronic warfare and cyber warfare have relatively fast learning curves. Measure begets countermeasure begets counter-countermeasure and so on. But the cycles in cyberwar are faster and likely to lead to a permanently *lower* plateau of efficacy for the attacker. In cyberspace, the first attack is most likely to have significant effects, particularly if the attack itself is a strategic surprise (e.g., the preceding weeks were uneventful) so

that affected systems are operating in peacetime mode. Even if the attack were carried out against an alerted adversary, the possibility that the attacker knows of specific vulnerabilities that the defender overlooked means that some attacks may well get through. *After* the attack, however, the defender will realize that some of its systems were too exposed to the rest of the world or at least its other networks. It may well figure out the specific vulnerabilities that allowed such attacks to take place and fix or route around them. It will have a more nuanced understanding of how far to trust each of its information systems. As a result of all this, a second wave of attacks is likely to hit a higher wall, and less is likely to get through. The same logic of diminishing returns would characterize a third or fourth wave and so on. Thereafter, successful attacks tend to be those that would exploit newly found vulnerabilities—particularly in just-fielded systems.

Cyberwar as Strategic War

If cyberwar is going to assume strategic importance, it must be able to generate effects that are at least comparable to, and preferably more impressive than, those available from conventional warfare.[4] Can it?

There is a wide range of opinion on that score. People have worried about cyberwar for most of the last 20 years, and in all that time, not one person is known to have been killed by a cyber attack.[5] As for damage, estimates vary widely from several hundred million dollars a year to several hundred *billion* dollars a year. The most costly single attack was probably the "I Love You" virus in 2000, whose costs have been estimated at as much as $15 billion but which may be more realistically estimated at several hundred million dollars, if that.[6] Only one power plant is known to have been disabled by hackers—a system in southern Brazil in 2007—and even there, the power outage has been disputed by local authorities as soot buildup. The only two examples of a state's using cyber attacks against another were Russia's attacks against Estonia in 2007 and Georgia in 2008 (and Russia's responsibility is questionable in the first case); both caused disruption that can be measured at no more than the low millions of dollars, and both pulled their victims closer to rather than pushing them farther from NATO. The Stuxnet worm, if it worked, did serious damage, but it was closer in form to a onetime act of sabotage.

The depletion dynamic noted above would work in roughly the same way in the civilian world as it does in the military world. These days, networks

and systems are established with some degree of security adequate only to deal with the day-to-day threats such institutions face. Banks, for instance, give a great deal of thought to security in large part because the motive to rob them is ever present. Bank security is fairly good; bankers can reduce the damage to acceptable levels, which also puts a top bound on the damage a state-sponsored bank thief could carry out. Electric power companies, by contrast, are rarely attacked—what would be the point? Thus, unless they have been prodded to isolate themselves by the deluge of threat scenarios over the last few years, the difference between a state-level threat and today's threat could be quite substantial, and they may not necessarily be so well prepared. But, should state hackers appear, many such institutions would learn quickly that the threat environment had changed and, with more time, how to survive and cope with such change. Coping with the worst attacks might be expensive and disruptive. But, at the very worst, the most primitive response (sever all Internet connections) would return the US economy to the state that it had in the mid-1990s, before networking became so ubiquitous. Being cyber-bombed back to the 1990s has its downside, but it hardly compares to being bombed back to the Stone Age (pace LeMay) by conventional weaponry.

More to the point, for cyber to be a strategic weapon for coercive purposes, it has to be frightening to the population at large, or at least to their leaders—so frightening that the aggressors can actually reap some gains from the reaction or concession of their targets.[7] One motive for strategic cyberwar may be to threaten its use to modulate an ongoing conventional war—but that requires the effects of a cyber attack to be significant relative to the cost, casualties, and damage of violent conflict. Another may be straightforward coercion prior to a war. Imagine a scenario in which Taiwan declares its independence; the Chinese plan to take the island but want to forestall US intervention. China takes down power in a few US metropolitan areas as a way of suggesting that it can do worse (merely threatening to take down power may be much less impressive and hence less dissuasive, given the great uncertainties in what any given attack can do before one is demonstrated). So, would the United States accede to China's invasion of Taiwan? Or instead, would it regard the Chinese threat to be a strategic threat and thus regard the China-Taiwan struggle as strategic rather than local for having become entangled with that larger threat? US reactions to Pearl Harbor and 9/11 suggest the latter. Our strategists, in

turn, should not blithely assume other countries can be rolled even if we cannot be—those other countries can also be quite stubborn.

It follows that if the use of cyber weapons is unimpressive at the strategic level, the fear that might come from the *threat* to use cyber weapons may be similarly unimpressive. It is difficult to make credible threats because the efficacy of cyber weapons is strongly, perhaps overwhelmingly, determined by features of those systems such weapons are targeted against. Once such weapons are used successfully, their credibility goes up, but then the attacker (as well as the target) has to deal with the consequences of their *use* (e.g., open hostilities). Such consequences will complicate and may overwhelm the purely coercive/deterrent effect of threatening *subsequent* use.

Fear, Uncertainty, and Doubt

While the preceding discussion may create doubt about the strategic impact of cyberwar, there are other considerations with perhaps more long-term resonance. Consider the oft-conflated trinity of FUD: fear, uncertainty, and doubt.[8] Nuclear arms fostered fear, but there was not a great deal of doubt or uncertainty in their applications. Cyber may be the opposite—incapable of inducing real fear directly, but putatively capable of raising the specter of doubt and uncertainty. It can do so immediately by scrambling the data upon which decisions by man or machine are made. Its specter can do so latently. Inherent in the possession of consequential vulnerabilities is that their owners are unaware exactly which ones exist and what effect their exploitation may have—otherwise they likely would not be vulnerabilities for very long. It is virtually impossible to prove that any particular complex system exposed to the outside world (e.g., via the Internet) is not invulnerable or even uninfected. For all anyone knows, some code in such a system could be waiting for an explicit command or some internal circumstance (e.g., reaching a certain date/time or receiving a particular message) to force the system to fail. If there is an attack, the name of the attacker may not be known, much less its motive or purpose.

Keeping that point in mind, now backtrack to the dawn of the nuclear era. Until then, one could envision any state being disarmed and destroyed by another. Afterwards, it was impossible to conceive of a nuclear-armed state being destroyed (except by another willing to sacrifice most of itself

in the bargain), much less occupied. The most operationally offensive of weapons turned out to be the most strategically defensive weapon ever created. Ever since, the effective point of such weapons, to adulterate the famous phrase of Bernard Brodie, has been not to use them but to brandish them to make a point, to tell a story, as it were, about what were and were not a state's vital interests. In a mature strategic environment, the role of nuclear weapons was to become an element of narrative. The advent of terrorism and insurgency in the postwar era has strongly reinforced the role of narrative. Terrorism bills itself as the propaganda of the deed. Insurgency is currently local politics by other means. They are meant to lower the population's confidence in its own government. They, too, tell a story. Conversely, the primary thrust of US counterinsurgency doctrine is the use of armed forces to bolster such confidence—a different story.

Putting the two together sets the stage for delineating the purpose of *strategic* cyberwar. It, too, illustrates a narrative. There are many possible narratives available; many clearly have to do with confidence. A cyber attack that disables some infrastructure says as much about its reliability—the reliability of those who own, operate, or stand behind such infrastructures—as a physical attack. Those who would corrupt a state's banking system make a statement about the creditworthiness of the state and its citizens. The persistent presence of a cyberwar capability, if irritating enough, serves to taunt institutions. All this assumes, of course, an adversary talented enough and a set of system owners feckless enough to give credence to such a narrative.

The United States, for its part, generally has little interest in creating chaos or ruining the authority of other institutions, even if some regimes deserved as much. Societies that depend on cyber systems understand the risks of starting *that* fight.

Nevertheless, a US capability for offensive strategic cyber operations may actually be worthwhile. Start with the observation that a military that can collect, analyze, distribute, and make decisions on the basis of copious information is likely to do much better in combat than one that cannot. Such a vision has been increasingly demonstrated over the last 20 years, starting with the first Gulf War, wending its way through Bosnia, and culminating with Operations Allied Force, Enduring Freedom, and Iraqi Freedom. Even in today's difficult counterinsurgency environment, the advantages of networking remain. They allow time-urgent targeting and enable forces to learn faster from the experiences of one another.

Presumably, it would run counter to US interests for countries potentially hostile to the United States to pursue a similar strategy, one that becomes more attractive the more powerful information technology becomes. Might developing an offensive cyberwar capability be a way to induce hesitation in *their* efforts to lay a network foundation under their war fighting?

Here is where an uncertainty-and-doubt strategy comes into play. How would other states react to the idea that the United States—and it need not necessarily be us—could have hacked into their military systems and implanted code into their communications systems and perhaps even their weapons systems? Such code would lie dormant until precisely such time as the target state wishes to use its military—at which point the code is unleashed: communications cease to work reliably, messages sent across the network may or may not be authentic, the ability to keep state secrets or even operational details cannot be guaranteed. Weapons relied on to make war could fail. Even if no such code has been embedded beforehand, so much information could have been collected about target systems that hackers can reliably enter and confound such systems in time of crisis.

If systems of both sides have been corrupted, both might be embarrassed before third parties (to include potential adversaries looking for signs of weakness) by their mutual inability to carry out military operations. Perhaps the hacker picked sides—in which case, the correlation of forces on the battlefield will be far worse than the target state had anticipated. If the target state believes (1) that it has been so hacked, (2) it has no alternative but the systems and equipment it has, (3) its estimate of war's outcomes are decidedly worse as a result, and (4) it does have a choice on whether to go to war, then one might conclude that its desire to go to war would be reduced. Under these circumstances, the uncertainty-and-doubt strategy would have achieved the aims that only fear could accomplish in the nuclear context. War is inhibited.

How might such doubt and uncertainty be induced? The most straightforward way is to hack into such systems and then make it obvious that they have indeed been hacked. Exactly who would do such a thing is secondary, since the point is not to emphasize US prowess but the vulnerability of their systems—indeed any such systems—to cyber attack. If the point is to provide not proof but uncertainty, then making the result obvious beforehand is unnecessary. In fact, it may be unwise. Proving that the other side may be vulnerable requires revealing the vulnerability. But every exposure

leads to fixes, which makes the next exploitation much harder. Thus proving a system was, is, and remains forever hacked may be impossible. However, the hint of an attack leaves no specific trace and, hence, no specific fix. General fixes, such as selective disconnection or the installation of anti-malware guards, may be employed, but there will be nothing that suggests which of these general fixes will do the job. After all, it takes twice as long to find something as it does to find nothing—and that is only true if one believes that sweeping a space and finding nothing proves that nothing is there; if finding is conclusive but sweeping and finding nothing is inconclusive, then it takes far longer than twice as long to find something as opposed to not finding something. It may not be possible to be confident once some supposedly rogue code has been found, even after a great deal of effort has been put into the quest, particularly because it is never clear exactly what would distinguish unexplained code from the rogue code an adversary could plant. Such code could be a glitch unrelated to any malevolent actor. Arthur Clarke's tenet—any sufficiently advanced technology is indistinguishable from magic—applies here. It helps that many foreigners have convinced themselves that US intelligence agencies are omniscient. US cyber warriors need never single out the target of their magic, but just ensure there are enough hints out there that say they do, in fact, possess the requisite skills. For all anyone knows, foreigners actually believe as much of our cyber warriors, and any testable hint in that direction could fail and blow the fairy dust from their eyes. It cannot be overemphasized that the target of the attack is not the system but *confidence* in it or, indeed, any system.

The vulnerability of third-world states to such magic is enhanced to the extent that they have to purchase (or steal the plans for) their military systems. To be sure, there have always been advantages to rolling your own or at least being as sophisticated as those who supply you. Usually, though, the difference is a matter of degree rather than direction. The more sophisticated countries tend to be adept operators of their own equipment; unsophisticated nations, less so. Thus, an F-16 in the hands of an American pilot is likely to be more effective than in the hands of a typical third-world pilot. More analogously, an F-16 that is maintained by the United States is apt to be in better condition than a similar plane maintained by a third-world military. But even an inexpertly flown and indifferently maintained F-16 is a war machine.

When it comes to information systems, however, a cyberwar system of positive value in US hands could become a system of less positive value in the hands of a hostile third-world state, even a distinctly negative value. States that purchase sophisticated information technology need to know not only how to use and maintain it, but also how to defend it against cyber attack. The failure to defend may mean that such systems, under pressure, leak information, drop out unexpectedly, or provide misleading data to war fighters and other decision makers—with consequences that may be worse than if they had never bought and grown dependent upon such systems in the first place—particularly if the more-sophisticated networked system replaced a less-sophisticated stand-alone system. In information systems, quality has a quantity all its own. A great hacker is likely to be orders of magnitude more efficacious than a merely good one, in ways that do not characterize the difference between a great hardware repairman and a merely good hardware repairman. The inability of third-world countries to generate great cyber warriors may be attributed to poorer educational facilities and a less-educated recruitment base. Yet, their lack of access to others' source codes or their not having built any of their own (and having few among them who have ever built any operational source code) helps ensure their military systems are far more vulnerable to cyber attack than comparable systems of sophisticated states.

A state faced with such fears may try to manage by pursuing compensatory strategies. For instance, states may observe that the effects of cyber attacks are temporary and difficult to repeat. They then maintain their investment strategy after reasoning that even if their weapons do not work when first used, they can survive the initial exchange and gain requisite military value from their weapons on the second and subsequent rounds. If so, they would have to overlook the ability of high-technology militaries to conclude successful conventional campaigns over the course of days rather than months or years. That is, they may not get a second round. A sophisticated system owner may be able to find and patch a newly exploited vulnerability within hours or days after it has been discovered when the entire world is helping. But can an unsophisticated system owner, on the outs with the developed world, countering a sophisticated US cyber attack count on so quick a recovery? The state may also realize that once a system has become ill, war fighters may not want to bet their lives on it until it has been completely cured (a far lengthier process) rather than simply having its symptoms relieved.

If states anticipate that their networked systems may be penetrated, they may elect to foreswear the development of network-centric warfare. Why try to face foes with weapons that may well fail spectacularly if used? Why not rely on lower-tech weapons that are robust against cyber attack because of no network connections and perhaps not even much electronics? So, is an uncertainty-and-doubt strategy thereby defeated? Au contraire, it has triumphed without even requiring hackers to validate their skills. But, would success in dissuading a potential adversary away from a high-technology challenge to the United States actually be in its best interest? A great deal depends on the kinds of wars the United States wants to deter and/or conduct. If the goal is to make it very difficult for others to carry out a conventional invasion or mount a conventional defense, low-technology forces are no match against what the United States has—even if they have given US ground forces fits in Iraq and Afghanistan. Abjuring quality may provide others the means to pursue quantity, but so far, the trade-off for others has not been particularly good; quality done right usually triumphs.

Alternatively, states beset by uncertainty and doubt may load up on the electronics and double-check their bona fides against supply chain attacks but abjure networking. Or they may network their machines but not their war fighters, limiting a possible vector of cyber attack but preserving a high-tech edge. If so, the real question is whether they have given up something of real war-fighting advantage to retain sufficient confidence in the electronics they *do* buy. At that point in the argument, one must yield the podium to proponents of network-centric warfare to make their case. A great deal depends on how much war fighters gain by reaching out to one another to gather the knowledge required to wage war and learn from war's experience.

Does not Stuxnet prove that cyberwar is real rather than a narrative? A great deal depends on what the worm actually succeeded in doing. Although people understand how it worked, nearly everything else about it remains a mystery: who wrote it, for what end, and with what effect?[9] The most common (current) explanation is that the Israelis intended for it to get into and confound or destroy components in Iran's Natanz nuclear fuel centrifuge plant. Iran's reaction, however, merits note. Although Iranians initially denied that anything in the Bushehr nuclear power plant was affected by the worm, they arrested several individuals associated with the plant in the weeks after the worm attack and accused them of being spies. Given the stories that a Russian contractor may have been the initial injection

point for the worm, it may well have affected their ability to trust and thus work with such contractors. If Stuxnet did nothing more than make Iranians lose confidence in their nuclear projects, it may well have succeeded even if it "failed."[10]

With all this, the broader narrative stands. The information revolution has created new and radically more-effective ways of going to war. The United States has exploited these advantages. But network-centric warfare comes at a price, and that price is vulnerability to cyberwar. In essence, there is a new game, but it is one played at a very high level. Those who cannot play at that level may want to think twice about entering the game at that level—indeed about entering the game at all.

Such is the case for developing offensive cyberwar capabilities to inhibit the investment strategies of rogue states and others who would contest the United States militarily. Would such a strategy apply to Russia and China?

With Russia, the best answer is almost certainly not, for two reasons. First, Russian capabilities at cyber warfare are very advanced—as befits a state as interested as it has been in *maskirovka* and as blessed as it has been with a surfeit of world-class mathematicians. They may fear our capabilities but are unlikely to regard them as magic. Second, Russia's military long suit is *not* systems integration of complex electronics and networks. It is precisely because they lack confidence in their conventional military that they lean so heavily on their nuclear arsenal. Thus, it is unlikely that their investment strategy would be diverted by the United States' development of cyber weapons.

With China, the best answer is most likely no. The Chinese have certainly shown enthusiasm for cyberwar. It shows up in their doctrine and in the great volume of intrusions people attribute to them. In contrast to Russia, however, it appears that Chinese talents in cyberspace lean more toward quantity (as befits a focus on cyber espionage) than toward quality (as would be required to get into hardened military systems). Furthermore, China's military investment strategy is quite different from Russia's. It has less interest in achieving nuclear parity and more in pursuing antiaccess strategies that rely on sensors, surveillance, and missiles—which normally require high levels of systems integration, hence, networking. These factors leave some—but only some—scope for a US dissuasion policy based on cyberwar capabilities.

What of the reverse—can others use the threat of cyberwar to deprive the United States of the confidence it needs to pursue network-centric

warfare? True, the US military worries—a lot—about how the cyberwar capabilities of other states may undermine its own plans.[11] Indeed, the possibilities were raised 15 years ago,[12] although at that point the fears were more notional than real. But the United States realistically has no better path other than going forward. The actual dominance of network defense in the resourcing of the US Cyber Command says as much. The DoD is prepared to spend billions, perhaps tens of billions, of dollars in pursuit of information assurance, precisely because it has little alternative.

Inhibiting Economic Growth?

Although the prospect of cyber attack might also be used to inhibit similar investments in digitizing the civilian commercial economy, the nature of the threat is different. Militaries exist against the day that they are most needed. Economies work from one day to the next. So, the possibility that the threat of cyberwar might inhibit investment in networking is unlikely to apply to commercial systems. First, such systems are used often and are attacked often as well, usually by criminals and amateurs, giving their owners confidence they work most of the time. By contrast, one only knows whether military systems work when used in war, which is contingent and infrequent (training is different, because there is little advantage to the enemy in making such systems fail temporarily). Second, there is a global infrastructure of corporations that supply, service, and maintain commercial information systems of sufficient diversity and experience that one can have confidence in their work. Military systems, in contrast, are more likely to be indigenously maintained, particularly if the owner is shunned by the West or if turnkey product support is contingent on good behavior. Third, the rationale for deepening the digitization of commercial and civilian systems is fairly straightforward and can be constantly validated in the day-to-day marketplace; cyber attacks constitute one risk that has to be factored into using them. The rationale for military digitization, especially by countries less involved in combat is far more speculative; there is a great deal of faith and emulation going into such decisions. By contrast, the effects from relying on digitization and then losing everything in a cyber attack when most needed—even if only for a few days—could be catastrophic.

Concluding Thoughts

In the 1970s, Thomas Wolfe "discovered" that modern art had "become completely literary: the paintings and other works exist only to illustrate the text."[13] Aesthetics aside, one can argue that cyberwar may have assumed a similar status, at least those acts of cyberwar that do not directly support military operations. It has become the latest manifestation of a trend that, when it comes to the means of war, what you do with it has become less important than what you say with it. Thus, the nuclear era was all about deterrence not combat, while more-modern cyber-limited conflicts are meant to serve as warnings. Building up our offensive capabilities is a confidence game. It says to those who would compete in our league: are you confident enough in your cyberwar skills that you can build your military to rely on information systems and the machines that take their orders? SSQ

Notes

1. For greater explanation, see Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), chap. 2.

2. Depletion (of cyber tricks) could mean one or more of several phenomena: (1) there are only so many tricks and they have been exhausted or (2) the best tricks have been played but what remain (a) produce results that are less useful or easier to recover from before much has been damaged, (b) work with less likelihood, or (c) work under fewer circumstances whose occurrence is less likely (e.g., the target machine is not in the required state very often). Alternatively, the time required to find the next good trick grows steadily longer.

3. One major exception is a cyber attack on a system that has yet to work correctly and thus has no proven set of correct instructions and hence no baseline to return to.

4. Inasmuch as nuclear weapons could end life on Earth and cyber weapons cannot, relegating cyberwar to, at best, a second-level strategic weapon seems to be an easy assertion.

5. Eleven people were said to have died as a result of the Northeast power outage in 2003. The outage was reportedly hastened because the Slammer worm disabled warning systems at First Energy, but subsequent investigation has largely discredited the connection.

6. The best guess may be more than 10 million individuals lost about an hour's worth of productivity. Evan Hansen, "Poll finds few affected by 'I Love You' Virus," *cnet.com*, http://news.cnet.com/Poll-finds-few-affected-by-I-Love-You-virus/2100-1023_3-241539.html.

7. The attacks of 9/11 seem to have liberated many strategists from having to ask what advantage attackers would reap from their actions—saying "they do not like us" seems to suffice. That noted, there has yet to be any act of cyber terrorism that has gone beyond defacing websites.

8. This term was coined by Gene Amdahl, after he left IBM to found his own eponymous company, to refer to the "fear, uncertainty, and doubt that IBM sales people instill in the minds of potential customers who might be considering Amdahl products."

9. Note how it took at least three corporations—VirusBlokAda (a security firm based in Belarus), Symantec (a US security firm), and Siemens (a manufacturer of industrial electronics)—

to contribute important pieces to determining how Stuxnet worked and how to ensure that copycats would not.

10. Iran's leader reported that centrifuges at Natanz were damaged. Thomas Erdbrink, "Ahmadinejad: Iran's nuclear program hit by sabotage," *Washington Post*, 29 November 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112903468.html. This, after months of denial, lent credence to the claim that Stuxnet did what it was designed to do but is no proof if one believes that Iran's leadership saw political advantage in blaming others for their own mistakes.

11. William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 97–108.

12. David Alberts, *Defensive Information Warfare* (Washington: National Defense University Press, 1996).

13. Thomas Wolfe, *The Painted Word* (New York: Bantam, 1977). The *Harper's* magazine article that excerpted the quotation begins nicely with his trip to an art exhibit in which, as one might expect, the pictures are large and the description-cum-explanation next to them are the size of a note card. He concludes by saying that if modern art were properly understood, the explanations would be wall-sized and the painting itself the size of note cards, merely an illustration of the narrative.