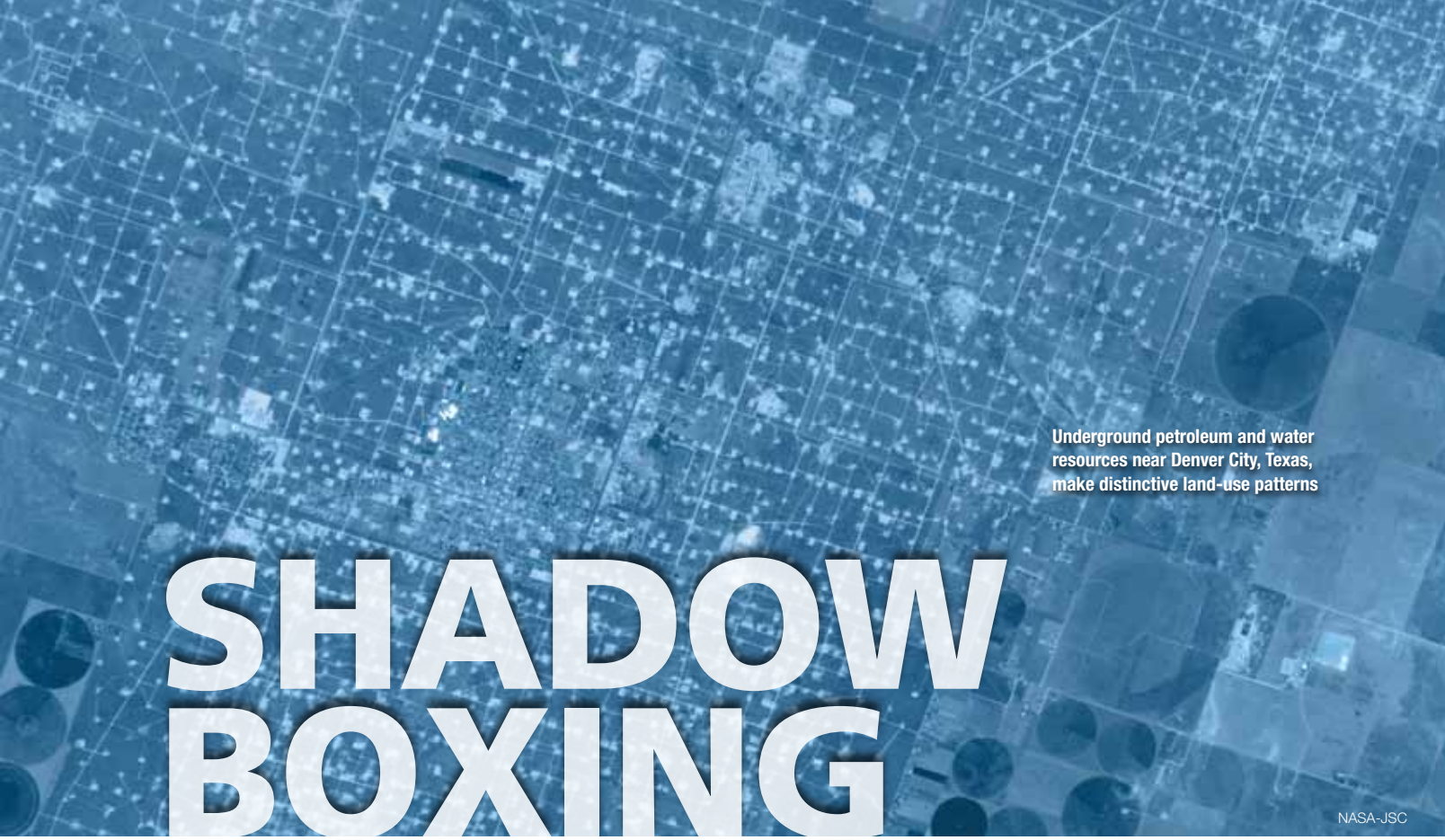

Underground petroleum and water resources near Denver City, Texas, make distinctive land-use patterns

NASA-JSC

SHADOW BOXING

Cyber Warfare and Strategic Economic Attack

By SOREN OLSON

First attack the enemy's strategy, then his alliance, next his army, and last his cities.

—Sun Tzu, *The Art of War*

U.S. critical infrastructure and resources are open to assault by "clever and persistent" cyber attacks. Such attacks could dramatically affect the supply chain of our most strategic resource, petroleum. Two decades of warnings concerning cyber vulnerabilities inherent in U.S. infrastructure have effectively gone unheeded. Bureaucratic constructions such as U.S. Cyber Command (USCYBERCOM) create the illusion of security but do not address the true problem. As we focus on creating effects in the enemy, we largely ignore the effects the enemy can create in us. Our culture of strategic fads (for example, hybrid war, fourth-generation warfare, irregular war, counterinsurgency, and counterterrorism) and our force-centric threat assessment indicate that changes in the character of war and corresponding implications may be missed. The character of war now undeniably involves attacks against economic and domestic infrastructure and cyber methods will be the weapons of choice.

Lacking the flashy nature of weapons systems, protection of domestic infrastructure and economic systems does not command a sufficiently high priority in strategic planning. While the Department of Defense (DOD), Department of Homeland Security, and other parts of the U.S. strategic community have begun to respond to the threat posed by cyber warfare, more needs to be done. Action must be taken despite domestic infrastructure and economic systems being run by civilians and outside traditional DOD jurisdiction.

Further complicating the issue of jurisdiction is the Stuxnet program. Stuxnet demonstrated conclusively that nationally developed cyber weapons are being directed at civilian targets in order to achieve strategic effects. Moreover, with two of the three major exploits in the Siemens software that Stuxnet attacked remaining unpatched several years later, the willingness of private companies to protect critical infrastructure systems is called into question.[1] These two observations combine to suggest that cyber warfare will not respect traditional institutional responsibilities. Indeed, one must wonder if it might be unwise to leave defense against strategic-type attacks—by foreign nations and others—to private companies and the domestic security apparatus.

Many authors use pre- and post-9/11 to characterize a shift in a how terrorism was viewed. Prior to September 2001, terrorism was largely seen as a criminal behavior.[2] After the impact of terrorism was demonstrated, it became a matter of national defense. Similarly, cyber security must be thought of in terms of before and after Stuxnet; the tendency to view the use of cyber weapons as criminal must be replaced with a view that sees their use against any U.S. interest as a hostile act.

Second Lieutenant Soren Olson, USAF, is a graduate of the Department of Military and Strategic Studies at the United States Air Force Academy. He is currently undergoing pilot training at Columbus Air Force Base.

DOD (Cherie Cullen)

Commander, U.S. Strategic Command, General C. Robert Kehler

Evolution of a Weapon

Of the challenges facing U.S. strategists, the tendency to dismiss vulnerabilities inherent in domestic infrastructure is likely the most insidious. The hubris with which cyber vulnerabilities are viewed is well illustrated by the following:

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.[3]

U.S. domestic infrastructure is dependent on cyber technologies,[4] and dismissing or limiting the cyber threat to existing concepts of warfare will ensure we are unprepared and unlucky.

Many assert that advances in technology fundamentally change our world. Similarly, when new technologies, weapons, and tactics are observed, many strategists call them revolutions in military affairs (RMA). These RMAs are asserted to change how warfare is conducted.[5] Regardless of RMA's utility as a concept, some developments in warfare such as technology, weapons, or methods have altered the character of war. Cyber warfare is one of these.

Change in the character of war is always noticeable after the fact, but the development of the technologies and methods that are the basis of the change is not. The roots of shifts in warfare are often present and undergoing development for years prior to their first decisive employment. Use of railroads, telegraphic communications, and headlong assaults into fortified positions during the Civil War foreshadowed operations in World War I.[6] The Germans tested coordination of ground and air elements in the Spanish Civil War, years before it was employed on a large scale against the Polish and French in World War II.[7] Similarly, the Yom Kippur War in 1973 used airpower to pin and hammer ground formations—a technique that would be used nearly 20 years later in Operation *Desert Storm*.[8] In each example, the years between initial development and large-scale implementation served only to increase the lethality of the final product. Cyber warfare has been developed and tested in a similar manner to these examples, and reports have consistently warned of the danger such warfare poses.

In 1991, the National Research Council stated, "Many disasters may result from intentional attacks on systems, which can be prevented, detected, or recovered from through better security."[9] The report called for a coherent strategy. Six years later, a Presidential committee noted that there was still no coordinating agency as had been previously recommended. Oddly, it asserted that contrary to the 1991 report, the nature of cyber threats was still poorly understood.[10] In 2001, arguments about the relative strengths of defense and offense in this new domain[11] were so indecisive that a congressional subcommittee recommended the cyber security of critical U.S. infrastructure and networks be left to the private sector.[12]

Advocates for relying on private industry to defend critical infrastructure should recall that businesses cannot always be relied on to serve national interests. Private companies are unquestionably patriotic and responsible, yet strategists must not forget the names of projects, companies, and people synonymous with short-term focus: the Ford Pinto, Enron, Fannie Mae/Freddie Mac, and Bernie Madoff. Nor can strategists discount the possibility of a private company intentionally leaving cyber vulnerabilities for its own

exploitation or at the direction of another national power. In light of these concerns, it would seem unwise to place the mandate of national defense on private industry, particularly when the stakes are high and the ability or willingness of companies to defend against cyber weapons, such as Siemens in the case of Stuxnet, is questionable.

Despite past errors, there is no question that U.S. cyber capabilities are increasing, particularly with the recent creation of USCYBERCOM. However, apologists for current cyber defense efforts should consider this recent assessment of U.S. cyber defense efforts by the Government Accountability Office:

U.S. Strategic Command has identified that DOD's cyber workforce is undersized and unprepared to meet the current threat. . . . It remains unclear whether these gaps will be addressed since DOD has not conducted a more comprehensive department wide assessment of cyber-related capability gaps or established an implementation plan or funding strategy to resolve any gaps that may be identified.[13]

Twenty years of disaster, investigation, and policy change have repeatedly led to the same regrettable outcomes.

Refinement of cyber warfare continued even as this dark comedy of concern and inaction played out. By 1999, one defense official stated the Federal Bureau of Investigation (FBI) was investigating some 6,080 daily attacks that were recorded on DOD computer systems.[14] In 2001, researchers at Dartmouth University predicted that cyber attacks would be the asymmetric weapon of choice for hostile groups and countries well into the future.[15] In 2003, the *Guardian* commented that U.S. Federal organizations were experiencing such a staggering number of cyber attacks on critical networks that the attacks were code-named "Titan Rain."[16] At this point, the Federal Government began pondering whether commercial cyber networks should be considered critical infrastructure and thus protected, but it took little significant action. A 2005 Presidential committee found that the "computers that manage critical U.S. facilities, infrastructures, and essential services can be targeted to set off system-wide failures, and these computers frequently are accessible from virtually anywhere in the world via the Internet."[17]

In March 2009, *Forbes* described a cyber espionage ring known as "GhostNet." GhostNet is thought to have infiltrated the government networks of 117 nations.[18] Such intrusions demonstrate the capability of foreign attackers to penetrate critical defended networks over long periods. Finally, the Stuxnet worm was discovered in July 2010 and is an example of cyber warfare coming of age. In a situation where traditional military attack was politically impractical, this complex series of 1s and 0s is asserted to have seriously damaged or even delayed the Iranian nuclear program.[19]

Despite its demonstrated capability to produce kinetic effects, the true significance of cyber warfare lies in its strategic application. Cyber warfare is ideally suited to Sun Tzu's definitive order of attack when engaging an enemy: "First attack the enemy's strategy, then his alliance, next his army, and last his cities."[20]

An adversary looking to attack the strategy of the United States should first determine what it seeks to protect. Security of energy supplies is the driving priority of current U.S. foreign policy, and trillions of defense dollars have been spent on maintaining access to Middle East oil supplies.[21] It is a cruel irony that in spite of this investment, persistent vulnerabilities in the oil supply chain demonstrate that the U.S. commitment to critical resource defense remains lacking.[22]

the anonymity of cyber warfare allows coordinated "submarine"-like attacks against the physical and cyber aspects of the U.S. petroleum supply chain

Crude Threat

As the world's largest consumer of petroleum, the United States is unable to supply its demand from domestic sources. Accordingly, some 36 percent of imports come from concentrated overseas routes and another 27 percent is transported into the continental United States via overland pipelines.[23] Even domestic petroleum depends on the domestic pipeline system. The ability to attack or defend this global and domestic petroleum supply network rests on computer systems.[24] Commercial guardians of critical resources, such as petroleum infrastructure, have been unable to even keep abreast with revealed vulnerabilities of supervisory control and data acquisition systems (SCADA).[25] They are not prepared for the onslaught that history dictates will be orders of magnitude greater than any cyber attack previously employed.

Historically, nations that import energy from sources prone to invisible attacks do not fare well. In World War II, U.S. submarines intentionally targeted Japanese petroleum imports.[26] After 2 years of invisible battering, less than 28 percent of oil shipped reached Japan.[27] Furthermore, the "loss of raw materials and petroleum and inability to transport items to the front lines lay at the heart of Japan's weakening ability to maintain effective military strength."[28] In the face of a sustained and coordinated attack, it is nearly impossible to completely defend an expansive network against an invisible enemy.

With cyber warfare, the true danger lies in the ability of an enemy to coordinate disparate actors and launch them against global interests while simultaneously attacking U.S. domestic petroleum infrastructure. In the late 1500s, England used privateers to attack the Spanish economy by raiding the gold-laden vessels sailing out of Central America. More recent examples are the American use of the Contras and mujahideen during the Cold War, as well as the Soviet support of Central American guerrillas. Among pawn employments, the Russian use of "patriotic" hackers against the Georgian banking and communication systems in 2008 is most applicable.[29] Each example points to the malleability of independent groups by a greater power.

The value of pawns in cyber warfare is that they further complicate attribution. A power can find and map vulnerabilities and then coordinate strikes using intermediaries. Past mapping of network and infrastructure vulnerabilities has not been treated as an act of war. Thus, while the source of information enabling the attacks may be known, so long as the originating hostile power uses pawns, there would be little direct action the United States could undertake.

Today, the spread of al Qaeda affiliates and other armed groups results in more pawns willing to attack American interests. This is the opportunity that a coordinating nation-state would offer such groups:

It should be clear that the energy infrastructure of the United States is its lifeblood, and as such,

it is one of the most critical of all infrastructures. The assets of the oil and gas industry are thus clear targets for economic jihad.[30]

Somali pirates are already using information from within shipping companies to seize vessels off the Horn of Africa.[31] These pirate groups have demonstrated a willingness to act on information received concerning the vulnerabilities of Western shipping companies. Modern pirates, armed with inside information, do token amounts of damage compared to the havoc an anonymous, malicious state actor could generate with a coordinated campaign. However, direct physical attacks augmented by information procured from cyber warfare are only one part of the threat: "The reliance on cyber technologies creates the opportunity for interrupted communications, false or misleading transactions, fraud, or breach of contracts, and can result in loss of service, loss of stakeholder confidence, or the failure of the business itself."[32]

Similarly, the anonymity of cyber warfare[33] allows coordinated "submarine"-like attacks against the physical and cyber aspects of the U.S. petroleum supply chain. The proliferation of armed groups along global shipping routes could allow an anonymous actor to coordinate an equivalent submarine campaign against the physical links of the global oil supply chain. This campaign of resource disruption would be aided by direct cyber attacks against the SCADA systems that run petroleum logistic hubs in the United States.

Logistics hubs serve as gateways for regional supply. They are characterized by interconnections among many pipelines and, often, other modes of transportation—such as tankers and barges, sometimes rail, and usually trucks, especially those used for local transport—that allow supply to move from system to system across counties, states, and regions in a hub-to-hub progression.[34]

When examining the layout of the U.S. petroleum infrastructure, concentration of pipelines run by SCADA systems at logistics hubs are clear domestic chokepoints. There are six primary hubs in the United States. These hubs are vulnerable to cyber sabotage directed either at the SCADA systems or the power grid supporting the hubs, as was demonstrated in 2007 when "an ice storm knocked out power to the hub in Cushing, Oklahoma, shutting down four crude oil pipelines [and] halting transport of roughly 770,000 barrels of oil per day."[35]

Though little known now, the 1982 U.S. cyber attack on the Trans-Siberian oil pipeline used a Trojan program that caused an explosion within the pipeline equivalent to a 3-kiloton weapon: "The U.S. managed to disrupt supplies of gas and consequential foreign currency earnings of the Soviet Union

U.S. Air Force (Lou Hernandez)

Anacortes Oil Refinery at base of Mount Baker, Washington

for over a year."[36] Though this example shows that cyber warfare's kinetic effects can be fearsome, such are not necessary to cause catastrophic economic damage.

Fear of Fear?

Deliberate attacks by a nation-state, using a combination of cyber weapons and traditional arms, have already been directed at economic targets. The addition of cyber means and economic targeting to the character of war was first demonstrated by the Russians:

When Russia invaded Georgia, a large portion of its military operations focused not on securing the areas inhabited by ethnic Russians but on Georgian ports and facilities for handling oil and gas. Unstable ground conditions, augmented by cyber attacks, soon made all of the Georgian pipelines seem unreliable. Meanwhile, 2 days after the invasion began, the Turkish section of the Baku-Tbilisi-Ceyhan pipeline was attacked by local militants, supposedly on their own initiative. One result of these developments was that BP Azerbaijan shifted its oil transport to the Russian Baku-Novorossiisk pipeline, even though the costs were double those of the Georgian pipelines.[37]

Cyber warfare was employed to leverage a target that was purely economic. BP shifted its oil contracts based on perception; physical compromise of the Georgian pipeline was not necessary. Due to the influence of perception, Georgia experienced serious economic damage with no physical destruction of infrastructure.

Given the ease with which economic damage can be inflicted on a single economic target, in this case a pipeline, one can see how the global system the United States relies on is at risk. Furthermore, proliferation of pawns would make it easy for a power to use them to coordinate attacks against the maritime routes and land-based logistic hubs used for transport of petroleum. Only a few of these attacks would need to succeed to undermine the foundation of the international energy system and reliable transport:

In 2007, total world oil production amounted to approximately 85 million barrels per day (bbl/d), and around half, or over 43 million bbl/d of oil, was moved by tankers on fixed maritime routes. The international energy market is dependent on reliable transport. The blockage of a chokepoint, even temporarily, can lead to substantial increases in total energy costs. In addition, chokepoints leave oil tankers vulnerable to theft from pirates, terrorist attacks, and political unrest in the form of wars or hostilities as well as shipping accidents.[38]

One commentator asserts that cyber attacks also look for "digital chokepoints," such as the electrical grid. As he explains, "Cyberspace is complex terrain, but the same idea obtains: squeeze a vulnerable throat."[39] Cyber warfare, like submarine warfare, is ideally suited to closing chokepoints. This approach was successfully employed by the United States against the Japanese; planners must anticipate a similar attack against the U.S. oil supply chain if only because of the potential for catastrophic damage. An incident that closed the Strait of Malacca even temporarily would reroute 50 percent of the world's shipping and cause further doubts about the reliability of energy transport. The potential economic damage from a coordinated cyber campaign executed on global oil chokepoints by a major power—or on domestic chokepoints—is inestimable.[40]

active defense for infrastructure systems would take years of development before they could be trusted to match modern offensive weapons

Shadow Puppets

Cyber weapons, potential proxies, and supply chain vulnerabilities all exist. What remains to be examined is what might motivate an actor to coordinate such a campaign. Sun Tzu and Carl von Clausewitz suggest what might cause such a campaign against U.S. petroleum supplies. First, consider Clausewitz's assertion that "Strong fortifications force the enemy elsewhere." Even in economic decline, the U.S. military has demonstrated its ability to fight in three conflicts on the opposite side of the world.[41] This military strength forces potential opponents to find a more effective angle of attack, such as a vulnerable supply line that provides a vital strategic resource. Second, the use of cyber against strategic resources is in accordance with Sun Tzu's maxim "to defeat the enemy without fighting and, when necessary, to win first, and then fight." These two concepts support the idea of removing a strategic resource via asymmetric and anonymous means. The example of submarine warfare in World War II, interdicting strategic resources, though not anonymous, demonstrates the ability of economic targeting by an invisible opponent to bring a great power to its knees.

However, the cyber warfare foreshadowed by Stuxnet and envisioned here would require resources in numbers that are available only to state actors.[42] Furthermore, such an indirect approach is distinctly contrary to typical Western strategy.[43] Whose hand should the United States expect to wield cyber warfare against its interests? It stands to reason that the nation with the clearest motive and intent is the most likely to challenge the reigning superpower.

The idea of using cyber warfare to strike at an unanticipated target, such as strategic resources, is perfectly in line with the Chinese concept of warfare known as *shashoujian*:[44] "Once strengths and weaknesses have been identified and assessed, the strengths can be avoided, and the weaknesses can be targeted for attack using *shashoujian*."[45]

Since 2004, China has conducted at least 14 major cyber attacks, including Titan Rain and GhostNet, on targets ranging from ExxonMobile and the German chancellor to Indian and DOD military networks.[46] The signs of weapon development have been noted, and the call for economic weaponization by Chinese experts has gone out: "It is only necessary to break with our mental habit of treating the weapons' generations, users, and combinations as being fixed to be able to turn something that is rotten into something miraculous."[47] The authors later give an example of what might be accomplished with such an approach:

On October 19, 1987, U.S. Navy ships attacked an Iranian oil drilling platform in the Persian Gulf. News of this reached the New York Stock Exchange and immediately set off the worst stock market crash in the history of Wall Street. This event, which came to be known as Black Monday, caused the loss of $560 billion in book value to the American stock market.[48]

Though this is an inaccurate claim, the validity of the statement is irrelevant insofar as the Chinese believe it is true.

Admittedly an attack by the Chinese against the international links of the U.S. petroleum supply chain would injure their own economy.[49] For this reason it seems unlikely they would attack international links except as a prelude to full-scale war with the United States.[50] However, the theory of economic interdependence should not be used as a shield to dismiss the possibility of economic cyber attack. Prior to World War I, the theory circulated that nations would not go to war as the economic devastation would be too great, yet it proved wrong.

Shadows' War

The destructive potential of cyber warfare in the economic, social, and physical realms demands that it be accorded the same level of respect and study strategists afford nuclear weapons. Defending against cyber attacks is like defending against nuclear weapons: attacks can take nearly any form and come from anywhere, and static defenses can be overwhelmed through mass or unconventional delivery. Unlike nuclear weapons, the anonymous and diffuse nature of cyber war may make deterrence impossible.

Further complicating successful defense is the proliferation of potential pawns that could be invisibly manipulated via cyber means. When this combines with the success of repeated enemy infiltration (Titan Rain), the global scope of infiltrations (GhostNet), and the kinetic effects (Stuxnet), no defense should be expected to withstand a coordinated cyber assault. Cyber warfare is well developed, and active defense for infrastructure systems would take years of development before they could be trusted to match modern offensive weapons. Active defense must not be the first focus. Instead, engaging in passive defense, evaluating vulnerabilities, creating backup systems, determining opponent cyber capabilities, and solving the attribution problem must take priority.

The problem of jurisdiction over cyber defense and the conundrum that DOD faces in the form of a mandate for national defense and a prohibition against domestic operations are not issues that can be solved by strategists. As the complications were created by national law, they can only be solved by national law. However, this inability to immediately fix a problem should not deter strategists from considering the uncomfortable implications of an infrastructure that is indefensible against modern cyber weapons and might not be reliable in case of limited or full-spectrum conflict.

We must recognize that while there are significant vulnerabilities among the links in the U.S. oil supply chain, they are but symptoms of a larger problem. Warnings about cyber warfare have been present for years, but reminiscent of another prominent defense failure prior to 9/11, actions taken remain insufficient. In light of these facts, we face the uncomfortable truth that China, as well as other nations, possesses a weapon, and our best defense against it amounts to boxing with its shadow. **JFQ**

NOTES

[1] Paul Roberts, "Many Stuxnet Vulnerabilities Still Unpatched," *Threatpost.com*, Kaspersky Lab Security News Service, June 8, 2011.

[2] Stephen D. Biddle, *American Grand Strategy after 9/11: An Assessment* (Carlisle, PA: U.S. Army War College Strategic Studies Institute, 2003), 25.

[3] Martin C. Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011), 134.

[4] *Cyberspace Policy Review* (Washington, DC: The White House, May 2009), 3, available at <www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

[5] Andrew F. Krepinevich, Jr., *The Military-Technical Revolution: A Preliminary Assessment* (Washington, DC: Center for Strategic and Budgetary Assessments, 2002, from Office of Net Assessment, 1992), 3, available at <www.csbaonline.org/wp-content/uploads/2011/03/2002.10.02-Military-Technical-Revolution.pdf>.

[6] Paddy Griffith, *Battle Tactics of the Civil War* (New Haven, CT: Yale University Press, 1989), 20.

[7] Rainer Waelde, *The Experience of the Japanese-Chinese War and of the Spanish Civil War for the Development of the German "Blitzkrieg Doctrine" and Its Lessons for the Transformation Process* (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2003), 25, available at <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA419865&Location=U2&doc=GetTRDoc.pdf>.

[8] Steven Baxter, "Arab-Israeli War October 1973: Lessons Remembered, Lessons Forgotten" (Master's thesis, Naval War College, 1994), available at <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA279557&Location=U2&doc=GetTRDoc.pdf >.

[9] National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: National Academies Press, 1991), 2–3.

[10] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, DC: The White House, October 1997), 78, available at <www.fas.org/sgp/library/pccip.pdf>.

[11] Professionals for Cyber Defense, letter to President George W. Bush, February 27, 2002, available at <www.uspcd.org/letter.html>.

[12] General Accounting Office, *Critical Infrastructure Protection: Significant Challenges for Developing National Capabilities,* report to the Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, U.S. Senate, April 2001, available at <www.gao.gov/new.items/d01323.pdf>.

[13] Government Accountability Office, *Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities*, report to Congressional Requesters, July 2011, available at <www.gao.gov/new.items/d1175.pdf>.

[14] "Guarding Cyber Pentagon," *CNN.com*, available at <http://articles.cnn.com/1999-03-05/tech/9903_05_pentagon.hackers_1_pentagon-computers-computer-attacks-computer-hackers?_s=PM:TECH>.

[15] Michael Vatis, *Cyber Attacks During the War on Terrorism: A Predictive Analysis* (Dartmouth, NH: Institute for Security Technology Studies, September 24, 2001), available at <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA395300>.

[16] Richard Norton-Taylor, "Titan Rain: How Chinese Hackers Targeted Whitehall," *The Guardian*, September 4, 2007, available at <www.guardian.co.uk/technology/2007/sep/04/news.internet>.

[17] President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization* (Arlington, VA: National Coordination Office for Information Technology Research and Development, February 2005), 17, available at <www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.>

[18] Paul Maidment, "GhostNet in the Machine," *Forbes.com*, March 29, 2009, available at <www.forbes.com/2009/03/29/ghostnet-computer-security-internet-technology-ghostnet.html>.

[19] William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *The New York Times*, January 15, 2011.

[20] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford: Oxford University Press, 1973), 77–78.

[21] Daniel Yergin, "Ensuring Energy Security," *Foreign Affairs* 85, no. 2 (March–April 2006), 82.

[22] Walter Russell Mead, "The Serpent and the Dove," in *Special Providence: American Foreign*

Policy and How It Changed the World (New York: Routledge, 2002), 110.

[23] U.S. Energy Information Administration, "How Dependent Are We on Foreign Oil?" *Energy in Brief* (Washington, DC: Department of Energy, June 24, 2011), available at <www.eia.doe.gov/energy_in_brief/foreign_oil_dependence.cfm>.

[24] Ulf Lindqvist, "Securing Control Systems in the Oil and Gas Infrastructure," *Oil & Gas Processing Review* (London: Touch Briefings, 2005), available at <www.touchbriefings.com/pdf/1713/ACF1A57.pdf>.

[25] Roberts.

[26] Navy Department, *Section III: Japanese Anti-Submarine Warfare and Weapons*, War Damage Report, no. 58 (Washington, DC: U.S. Hydrographic Office, January 1, 1949), 8, available at <www.ibiblio.org/hyperwar/USN/rep/WDR/WDR58/WDR58-3.html>.

[27] W.J. Holmes. *Undersea Victory: The Influence of Submarine Operations on the War in the Pacific* (Garden City, NY: Doubleday, 1966), 425.

[28] Michel T. Poirier, "Results of the American Pacific Submarine Campaign of World War II," U.S. Navy, December 30, 1999, available at <www.navy.mil/navydata/cno/n87/history/pac-campaign.html#N_19>.

[29] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, 2, available at <http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>.

[30] James J.F. Forest, *Homeland Security: Protecting America's Targets, Vol. III: Critical Infrastructure* (Westport, CT: Greenwood Publishing Group, 2006), 136.

[31] Giles Tremlett, "This Is London—The Capital of Somali Pirates' Secret Intelligence Operation," *The Guardian*, May 11, 2009, available at <www.guardian.co.uk/world/2009/may/11/somalia-pirates-network>.

[32] National Petroleum Council, *Securing Oil and Natural Gas Infrastructures in the New Economy* (Washington, DC: Department of Energy, June 2001).

[33] U.S. Naval Institute and CACI International, Inc., "Cyber Threats to National Security: Symposium I—Countering Challenges to the Global Supply Chain," March 2, 2010, available at <http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf>.

[34] Allegro Energy Group, "How Pipelines Make the Oil Market Work: Their Networks, Operation and Regulation," a memorandum for the Association of Oil Pipelines and American Petroleum Institute's Pipeline Committee, December 1, 2001, 7.

[35] "Ice Storm Trips Power, Paralyzes Key U.S. Oil Hub," Reuters, December 11, 2007, available at <www.cnbc.com/id/22200736/Ice_Storm_Trips_Power_Paralyzes_Key_US_Oil_Hub>.

[36] Eric J. Byres, "Cyber Security and the Pipeline Control System," *Pipeline & Gas Journal* 236, no. 2 (February 2009), available at <http://pipelineandgasjournal.com/cyber-security-and-pipeline-control-system>.

[37] U.S. Cyber Consequences Unit (US-CCU), special report, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, available at <www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.

[38] Energy Information Agency, *World Oil Transit Chokepoints* (January 1, 2008), 1, available at <www.eia.gov/cabs/world_oil_transit_chokepoints/Full.html>.

[39] Austin Bay, "Grab the Planet By the Throat," *RealClearPolitics* (April 22, 2009), 8, available at <www.realclearpolitics.com/articles/2009/04/22/grab_the_planet_by_the_throat_96106.html>.

[40] Energy Information Agency, 4.

[41] Referring to Iraq, Afghanistan, and Libya.

[42] Holger Stark, "Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War," *Der Spiegel Online*, August 8, 2011, available at <www.spiegel.de/international/world/0,1518,778912-2,00.html>.

[43] Laurent Murawiec, "China's Grand Strategy Is to Make War While Avoiding a Battle," *Armed Forces Journal* 143 (November 2005), available at <www.armedforcesjournal.com/2005/11/1164221/>.

[44] Most commonly translated as "Assassin's Mace," it refers to the Chinese search for weapons that are undetectable prior to use and cause such damage as to make retaliation by the victim impossible.

[45] Jason E. Bruzdzinski, "Demystifying Shashoujian," in *Civil-Military Change in China: Elites, Institutes, and Ideas after the 16th Party Congress*, ed. Larry Wortzel and Andrew Scobell (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, 2004), available at <www.mitre.org/work/best_papers/04/bruzdzinski_demystify/bruzdzinski_demystify.pdf>.

[46] Richard Stiennon, "A Brief History of Chinese Cyberspying," *Forbes.com*, February 2, 2011, available at <www.forbes.com/sites/firewall/2011/02/11/a-brief-history-of-chinese-cyberspying/>.

[47] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Beijing: PLA Literature and Arts Publishing House, February 1999), 20.

[48] Ibid., 190.

[49] Unless the attack affected only the domestic U.S. petroleum distribution network.

[50] Nations that export oil or have little stake in the international system (Iran, Venezuela, Russia, and North Korea) could execute campaigns against all links of the supply chain with little self-damage; indeed, the resulting petroleum market instability might be economically advantageous to these actors.