CSBA

Center for Strategic and Budgetary Assessments

CYBER WARFARE

A "NUCLEAR OPTION"?

ANDREW F. KREPINEVICH

CYBER WARFARE:
A "NUCLEAR OPTION"?

BY ANDREW KREPINEVICH

2012

About the Center for Strategic And Budgetary Assessments

The Center for Strategic and Budgetary Assessments (CSBA) is an independent, nonpartisan policy research institute established to promote innovative thinking and debate about national security strategy and investment options. CSBA's goal is to enable policymakers to make informed decisions on matters of strategy, security policy and resource allocation. CSBA provides timely, impartial, and insightful analyses to senior decision makers in the executive and legislative branches, as well as to the media and the broader national security community. CSBA encourages thoughtful participation in the development of national security strategy and policy, and in the allocation of scarce human and capital resources. CSBA's analysis and

outreach focus on key questions related to existing and emerging threats to US national security. Meeting these challenges will require transforming the national security establishment, and we are devoted to helping achieve this end.

ABOUT THE AUTHORS

Dr. Andrew F. Krepinevich, Jr. is the President of the Center for Strategic and Budgetary Assessments, which he joined following a 21-year career in the U.S. Army. He has served in the Department of Defense's Office of Net Assessment, on the personal staff of three secretaries of defense, the National Defense Panel, the Defense Science Board Task Force on Joint Experimentation, and the Defense Policy Board. He is the author of *7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century* and *The Army and Vietnam*. A West Point graduate, he holds an M.P.A. and a Ph.D. from Harvard University.

ACKNOWLEDGMENTS

The author would like to thank Mark Gunzinger, Dr. Herbert Lin, Dr. Evan Montgomery, Jim Thomas, and Barry Watts for reviewing earlier versions of this report, and for their insightful comments, criticisms and suggestions. Thanks also are due to Simon Chin, Eric Lindsey, and especially Abigail Stewart for their superb research support. Of course, any shortcomings in this report, either through commission or omission, are the author's sole responsibility.

CONTENTS

EXECUTIVE SUMMARY

The Internet has experienced a breathtaking expansion over the past two decades, from a small network limited primarily to the scientific community to a global network that counts more than two billion users. With expansion came increasing applications for the Internet, which fed further expansion and still more applications, to include the rise of a cyber economy, financial transactions, widespread automated regulation of key control systems, an explosion in the sharing and storing of information (including highly sensitive information), and the emergence of new forms of electronic communication such as email and social networking, among others.

In addition to these manifold societal benefits, the cyber domain, like the physical domains of land, sea, and air, has proven to be no stranger to crime and conflict. The cyber economy, which includes multiple financial systems, has spawned cyber crime. Storage of sensitive information on networks has given birth to cyber espionage against governments and cyber economic warfare against businesses. And in periods of crisis or conflict states have been subjected to various forms of cyber attack at both the tactical and operational levels of war.

This report explores the question of whether we are on the cusp of a major shift in the character of warfare as military competition expands into the cyber domain. Specifically, it explores growing concerns among senior policy-makers and military leaders in the United States and in other major cyber powers that both state and non-state rivals will be able to execute cyber attacks that inflict prompt, catastrophic levels of destruction upon their adversaries.

Given the increasing reliance on information systems in general and access to the Internet in particular, critical infrastructure is growing progressively

more vulnerable to cyber attack. Senior leaders in the United States and abroad have expressed concern that the risks of a cyber "Pearl Harbor" are growing. Some have even likened cyber weapons' potential to inflict damage to that of nuclear weapons.

But are such concerns valid? While it is difficult to undertake an assessment of a form of warfare about which relatively little is known, this report attempts to make some progress in thinking about the issue. That said, its conclusions are necessarily tentative.

There is reason to believe that the potential exists for a cyber attack to inflict relatively prompt, catastrophic levels of destruction on the United States and other states with advanced infrastructures—*but only if one accepts a broad definition of what constitutes "catastrophic" destruction*. Cyber weapons appear to be capable of meeting the minimum definition of catastrophic destruction in that they could inflict "extreme misfortune" on a state, in the form of imposing very large, long-term costs. For example, by *repeatedly* disrupting critical infrastructure for short periods of time, cyber attacks could erode public confidence in the reliability of

said infrastructure. The costs of such attacks would be paid in terms of some or all of the following:

- *Accepting* the substantial economic losses inflicted by repeated attacks;
- *Adapting* the infrastructure at significant cost to substantially reduce the losses suffered in future attacks; or, in extremis,
- *Abandoning* reliance on information networks to manage and support critical infrastructure (i.e., returning to the pre-Internet era circa 1980).

Some of these costs are being incurred today, albeit at a far lower level than would be the case in the event of a large-scale cyber attack. Most countries and businesses are already accepting losses associated with cyber attacks as a cost of doing business. Some are working to adapt their systems to minimize their vulnerability at an acceptable cost, but few have abandoned their reliance on information networks.

In the context of the historical analogies discussed in this report, cyber weapon development appears to most closely approximate that of air power during

the 1930s. At that time the world had experienced several decades of progress in aviation technology, and had seen air forces employed in World War I and in lesser conflicts following the war. Yet none of these conflicts saw a major power employ the full force of its air power against another advanced state.

Comparatively speaking, we are at the same point with respect to cyber warfare. The cyber domain has been an area of competition between states and non-state entities for some two decades; cyber weapons have been employed in minor conflicts, and political and military leaders have made startling claims regarding the capabilities of these new weapons. But we have yet to see the cyber power of a major state employed in full force. As with air power in the 1930s, it is difficult to state with confidence just how effective cyber weapons will be, if and when they are employed against a society's critical infrastructure.

The concerns over a cyber "Pearl Harbor" are legitimate. Just as the attack on U.S. military facilities on December 7, 1941, shocked the American public, a large-scale successful cyber attack on the United

States would likely generate a similar sense of shock. However, just as the attack on Pearl Harbor did not inflict a decisive blow to the United States, neither is a surprise massive cyber attack likely to do so.

What seems clear is that, despite the assertions of some, *cyber weapons appear to have nowhere near the ability to inflict catastrophic destruction along the lines of a major nuclear attack.* There is little doubt that a major nuclear attack can meet the most demanding definition of "catastrophic": triggering the utter overthrow or ruin of a state and its society. By contrast, a cyber attack against critical infrastructure is almost certain to be *much less* destructive than a large-scale nuclear attack. Moreover, the attacker's confidence in a cyber attack's ability to inflict catastrophic destruction is likely to be *far less* than that of an attacker employing large numbers of nuclear weapons. Simply put, nuclear weapons remain in a class all their own. When it comes to discussions regarding inflicting prompt catastrophic destruction, nuclear weapons are the gold standard, whereas cyber weapons barely qualify for a place in the conversation.

This assessment finds that we are *far more likely* to experience major cyber attacks than we are nuclear attacks. There are several reasons for this:

ATTRIBUTION. Since World War II, states have refrained from employing nuclear weapons out of fear that such weapons might be used against them. This is deterrence through the threat of massive retaliation. This form of deterrence requires that the victim be able to identify the source of the attack. Yet attributing the source of a cyber attack is likely to remain both costly and difficult. To be sure, even the remote prospect of being identified might be sufficient to deter a risk-averse leadership from committing to a major cyber attack. But what of highly risk-tolerant leaders—men like Adolf Hitler, Josef Stalin, Mao Zedong and Saddam Hussein? For leaders such as these, the prospect of inflicting major harm on their enemies while avoiding retribution could prove irresistible.

Risk-tolerant leaders may also be tempted to engage in catalytic warfare in which they play the role of a third party covertly attempting to instigate or influence a war between two other parties. In a crisis

between two powers, if one were to suffer a massive cyber attack, the natural inclination might be for the victim to assume the other state party to the crisis is responsible. Circumstances such as these could provide another layer of insulation from attribution for risk-tolerant leaders.

Should a radical non-state entity acquire cyber weapons capable of inflicting large-scale destruction, there may be little if any restraint on their use. Such groups may care little about avoiding attribution; in fact, they may claim responsibility for an attack. As these groups have no infrastructure against which to retaliate it is not likely that deterrence through the threat of punishment will prove effective.

PROLIFERATION. There is also the problem of numbers. It is highly likely that many more states (and even non-state entities) will develop imposing cyber arsenals rather than nuclear arsenals. With many more decision-makers possessing these weapons, it cannot but increase the odds that they will be used.

The combination of large numbers of major cyber competitors—perhaps including non-state

entities—with highly risk-tolerant leaders suggests a significant potential for cyber proxy wars. While it is difficult to imagine a nuclear proxy war, this is not the case with regard to cyber weapons. The apparent willingness on the part of states to use proxies to better avoid attribution when stealing state secrets, intellectual property, and other valuable information could lower the barriers, especially for risk-tolerant leaders, to engage in large-scale cyber war against an enemy's critical infrastructure.

ABSENCE OF A CLEAR CYBER "FIREBREAK." In the case of nuclear weapons, they are either being employed or they are not; there is a clear firebreak between use and non-use. This is not the case with respect to cyber weapons. Thus it may be difficult for the leadership of one cyber power to determine when, in the mind of its enemy, it has crossed the line between cyber operations that are "acceptable" and those that will trigger a major escalation in the intensity of cyber activity that could lead to catastrophic attacks. The picture is blurred even further owing to the fact that states are constantly

under cyber attack from multiple sources, not just one. Matters are made murkier still by the similarities that exist between cyber reconnaissance operations and those designed to implant cyber weapons or conduct an attack.

In summary, the concerns of many senior leaders with regard to the dangers of a large-scale cyber attack appear to have merit. It seems likely that a major cyber attack that would inflict catastrophic damage on the critical infrastructure of an advanced economy is both plausible and much more likely to occur than a nuclear attack with the same objective. Even this kind of attack, however, would pale in comparison to the damage that would result from a major nuclear attack.

CHAPTER 1 > **INTRODUCTION**

The Internet has experienced a breathtaking expansion over the past two decades, from a small network limited primarily to the scientific community to a global network that counts more than two billion users. With expansion came increasing applications for the Internet, which fed further expansion and still more applications, to include the rise of a cyber economy, financial transactions, widespread automated regulation of key control systems, an explosion in the sharing and storing of information (including highly sensitive information), the emergence of new forms of electronic communication such as email, and social networking, among others.

In addition to these manifold societal benefits, the cyber domain, like the physical domains of land, sea, and air, has proven to be no stranger to crime and conflict. The cyber economy, which includes multiple financial systems, has spawned cyber crime. Storage of sensitive information on networks has given birth to cyber espionage against governments and cyber economic warfare against businesses. And in periods of crisis and conflict states have been subjected to various forms of cyber attack at both the tactical and operational levels of war.

This report explores the question of whether we are on the cusp of a major shift in the character of warfare as military competition expands into the cyber domain. Specifically, it explores growing concerns among senior policy-makers and military leaders in the United States and in other major cyber powers that there either currently exists or will soon exist the ability of state and non-state rivals to execute prompt cyber attacks that could inflict damage on their adversaries so as to produce catastrophic levels of destruction. Among the likely principal targets of such attacks are the electrical power

grid; energy supply (e.g., oil and gas pipelines); water desalination, purification, and distribution plants; and communications, transportation, and financial sectors.

THE ISSUE OF CATASTROPHIC DESTRUCTION

Critical infrastructure functionality is growing progressively more vulnerable to cyber attack, given its increasing reliance on information systems in general and access to the Internet in particular. Secretary of Defense Leon Panetta is among those sounding the alarm, declaring that:

> [W]hen it comes to national security, I think this [i.e., cyber warfare] represents the battleground for the future. I've often said that I think the potential for the next Pearl Harbor could very well be a cyber attack. If you have a cyber attack that brings down our power grid system, brings down our financial systems, brings down our government systems, you could paralyze this country.[1]

1 "Cybersecurity 'battleground of the future,'" *United Press International*, February 10, 2011, available at http://www.upi.com/Top_News/US/2011/02/10/Cybersecurity-battleground-of-the-future/UPI-62911297371939/, accessed on January 10, 2012.

General Keith Alexander, the commander of the United States' newly established Cyber Command, has echoed Secretary Panetta's concerns. In answering his own question of "What's technically possible?" in cyber warfare, he replied that an enemy could "Take down the power grid, the stock exchange, and the Internet—for awhile."[2] General Alexander also noted that this capability is not necessarily restricted to states, as "Attacks by hackers and criminals can cause 'nation-sized' effects."[3]

In a revealing article in the journal *Foreign Affairs*, then-Deputy Secretary of Defense William Lynn warned that cyber attacks could have catastrophic effects, stating:

> Hackers and foreign governments are increasingly able to launch sophisticated intrusions into the networks that control critical civilian infrastructure. Computer-induced failures of U.S. power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption.[4]

2 Keith B. Alexander, "Cybersecurity Symposium Session 1," keynote address, Cybersecurity Symposium, University of Rhode Island, April 11, 2011, YouTube video clip, between 1:17:23 and 1:17:35, available at http://youtu.be/gcEFcDqlQC0, accessed on April 10, 2012.

3 Keith B. Alexander, testimony before the House Armed Services Committee, September 23, 2010, p. 5.

4 William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010.

Similarly, the former Director of National Intelligence, retired Admiral Mike McConnell, took these statements to their logical conclusion in declaring that "The cyber-war mirrors the nuclear challenge in terms of the potential economic and psychological effects."[5] McConnell's linking of cyber and nuclear weapons finds some support from former-Vice Chairman of the Joint Chiefs of Staff, General James Cartwright, who stated, "I think that we should start to consider that regret factors associated with a cyber attack could, in fact, be in the magnitude of a weapon of mass destruction."[6]

Military strategists in other countries second these concerns over the potential of cyber weapons to boost military effectiveness. Russian Deputy Chief of the General Staff, Alexander Burutin, has spoken about how cyber warfare is changing the landscape of modern combat:

> [I]n the foreseeable future, achieving the ultimate goals in wars and confrontations will be brought

5 Mike McConnell, "How to Win the Cyberwar We're Losing," *Washington Post*, February 28, 2010.

6 James E. "Hoss" Cartwright, testimony before the United States-China Economic and Security Review Commission, "Hearing Before the U.S.-China Economic and Security Review Commission, March 29-30, 2007," March 2007, available at http://www.uscc.gov/hearings/2007hearings/transcripts/mar_29_30/mar_29_30_07_trans.pdf, accessed on March 13, 2012.

> about not so much by the destruction of enemy groups of troops and forces, but rather by the suppression of his state and military control systems, navigation and communication systems, and also by influencing other crucial information facilities that the stability of controlling the state's economy and Armed Forces depends on.[7]

General Burutin's assertion that cyber attacks will bypass an enemy's armed forces and strike directly at the foundation of a state's war-making potential recalls the great Italian air power theorist Giulio Douhet, whose predictions about the potential of air power to achieve decisive effects had to await the development of nuclear weapons before they could be realized.

Chinese military officers see the cyber threat in a similar manner, to include linking cyber weapons with nuclear weapons. For example, an essay by two People's Liberation Army (PLA) scholars, Senior Colonel Ye Zheng and his colleague Zhao Baoxian, in *China Youth Daily* stresses the importance of

7 Jeffrey Carr, Sanjay Goel, Mike Himley, Andrew Lasko, and Thomas J. Saly, *Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats* (McLean, VA: Grey Logic, 2010), p. 12.

China's cyber warfare capabilities, concluding that "Just as nuclear warfare was the strategic war of the industrial era, cyber-warfare has become the strategic war of the information era, and this has become *a form of battle that is massively destructive and concerns the life and death of nations*."[8]

Other PLA strategists see China's cyber arsenal as a strategic deterrent comparable to that provided by nuclear weapons but possessing greater precision, thereby enabling cyber strikes to induce far fewer casualties than nuclear strikes,[9] while also noting that cyber weapons possess a far longer range than any weapon in the PLA's arsenal, save for a few ballistic missiles. As early as 2007 Major General Li Deyi, the deputy chair of the Department of Warfare Theory and Strategic Research at the PLA's Academy of Military Sciences, stated that cyber deterrence is rising to the level of strategic deterrence

8 As quoted in Chris Buckley, "China PLA Officers Call Internet Key Battleground," *Reuters*, June 3, 2011. Emphasis added.

9 Bryan Krekel et al., *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (McLean, VA: Northrop Grumman, 2009), p. 20. Some describe cyber warfare as a form of "Acupuncture War," in which cyber weapons attack the critical points in a network that, much like the pressure points in martial arts, when taken out can shut down an entire system. Acupuncture War is designed to make "the first battle being the final battle." In this manner, Acupuncture War is similar to air power enthusiasts' vision that strategic strikes against an adversary's center of gravity would produce decisive results. See Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Waltham, MA: Syngress, 2011), p. 43.

and assuming a level of importance second only to nuclear deterrence.[10]

Given these statements by such a wide range of policy-makers and military authorities, the absence of a major cyber conflict may have less to do with a lack of cyber weaponry capable of conducting attacks that trigger catastrophic effects, and more to do with the absence of an attacker with the incentive to execute such an attack. If true, it means that the United States may be at grave risk of being struck by a major cyber attack with little or no notice—a "Cyber Pearl Harbor" to use Defense Secretary Panetta's analogy—with potentially dire consequences.[11] Given the size of its economy and its heavy reliance on computer networks, the United States arguably has more to lose in such a war than any other state, and certainly more than any non-state entity.

If these warnings prove to be justified, cyber weapons would join nuclear weapons (and arguably precision-guided munitions and biological agents) as the only other weapons with the ability to inflict prompt, catastrophic damage. Yet, despite

10 Andress et al., *Cyber Warfare*, p. 78.

11 Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: Harper Collins, 2010), p. 216.

its enormous potential consequences for the security and well being of the world's leading economic powers, the issue of catastrophic cyber attack is only now emerging, even though we are perhaps 15 years or more into the era of cyber weaponry and warfare. This stands in striking contrast to the concentrated and persistent efforts of many of the world's best strategic thinkers to understand the implications of nuclear weapons in the decades immediately following their introduction in 1945.

Why has it taken so long for these concerns to arise? After all, fears over the potential of nuclear weapons arose immediately with the employment of the first atomic bombs in July and August of 1945. Several possibilities seem plausible. One is that while Hiroshima and Nagasaki offered vivid demonstrations of the destruction even two relatively small fission weapons could accomplish, there has been no similar dramatic demonstration of cyber weaponry. Perhaps it is because cyber activity—ranging from crime to economic warfare, from espionage to support of military operations—has yet to produce catastrophic effects. It may also be that until recently

cyber weapons had not achieved the *perceived* capability to inflict the kind of damage attributed to nuclear weapons. Finally, given the level of secrecy associated with the cyber competition between governments, militaries, businesses, organized crime, and other non-state entities, it is difficult for independent observers to discuss the issue with anything approaching the level of confidence associated with that brought to bear by strategists in the decade following the introduction of nuclear weapons. Former CIA director, General (Ret.) Michael Hayden summed it up nicely when he observed that "Rarely has something been so important and so talked about with less clarity and less apparent understanding than this [cyber] phenomenon."[12]

FOCUS AND ORGANIZATION

This report focuses on two questions that arise from this growing chorus of voices linking cyber weapons with nuclear weapons as capable of triggering prompt, catastrophic destruction. First, are these concerns valid? Put another way: are cyber

12 Michael V. Hayden, "The Future of Things Cyber," *Strategic Studies Quarterly*, Spring 2011, p. 3.

weapons actually capable of creating catastrophic effects akin to those of nuclear weapons; i.e., effects that are both concentrated in time and difficult to remediate? Second, if cyber weapons are actually capable of achieving such effects, what are the strategic implications?

These questions are addressed in the chapters that follow. Chapter 2 provides a context for thinking about the matter of prompt, catastrophic destruction. It does so by tracing the rise of air power to the introduction of nuclear weapons.Chapter 3 offers a brief examination of the trends in threats to networks in the cyber domain over the past decade or so. It is provided primarily for those readers with a rudimentary background in the cyber competition.[13] Readers who are knowledgable in the basics of the cyber competition may find it useful to skip this chapter and move directly on to Chapter 4, which offers a preliminary assessment of the character of the cyber competition and its implications for strategy in general and the U.S. competitive position in particular. It then goes on to provide a brief

13 There is also a glossary of terms at the back of this report that may also prove useful to readers who are working their way up the cyber learning curve.

discussion of possible vulnerabilities in two critical infrastructure sectors: the power grid and financial system. Chapter 5 examines more closely the similarities and differences between cyber capabilities and nuclear capabilities. Chapter 6 provides a summary of the report's major findings and suggests areas for further research and analysis.

It should be noted that the results of the assessment that follows are somewhat speculative. This is in large part a consequence of the high level of secrecy associated with the cyber competition, which arguably exceed by a substantial margin that surrounding nuclear weapons, even in the years immediately following their creation.

CHAPTER 2 > AIR POWER, NUCLEAR WEAPONS, AND CATASTROPHIC DESTRUCTION

WHAT IS CYBER WAR?

The accelerating rate of advances in technology, combined with an increasingly unstable geopolitical environment, make the current period perhaps the most promising for broad, dramatic shifts in the military competition (i.e., a military revolution) since the era between the two world wars.[14] The so-called interwar revolution saw the advent of combined-arms, mechanized air-land operations

14 For a discussion of the military revolution that emerged between the two world wars, see Williamson Murray and Allan R. Millett, eds., *Military Innovation in the Interwar Period* (Cambridge, United Kingdom: Cambridge University Press, 1996). For an overview of military revolutions, see Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest*, Fall 1994, pp. 30-42. This latter work was based on three assessments of the military revolution (the so-called revolution in military affairs) undertaken by the author. The first of these assessments, produced for the Office of Net Assessment and under the direction of Andrew W. Marshall, was completed in 1992, and later published by CSBA in 2002. See Andrew F. Krepinevich, *The Military-Technical Revolution: A Preliminary Assessment* (Washington, DC: Center for Strategic and Budgetary Assessments, 2002).

(*blitzkrieg*), the displacement of the line of battle at sea by fast carrier task forces, the rise of long-range strategic aerial bombardment, and the introduction of integrated air defense networks. Later, World War II witnessed the introduction of nuclear weapons, as well as cruise and ballistic missiles, which triggered another fundamental change in the character of warfare. More recently, the First Gulf War witnessed the advent of precision-guided weapons warfare,[15] which produced an order-of-magnitude increase in the effectiveness of air power. That war also saw the onset of a rapid expansion in the U.S. military's reliance on space systems for a wide range of missions, from intelligence, surveillance, and reconnaissance (ISR), to target acquisition and tracking, guiding munitions to their targets, and providing battle damage assessment. In response, we have

15 Precision-guided weapons were first employed in large numbers during the Vietnam War; however, the first intensive use of such weapons occurred in the First Gulf War. During the period between February 1972 and February 1973, over 10,500 laser-guided bombs (LGBs) were dropped in Southeast Asia. (An Air Force study puts the number of LGBs dropped between April 1972 [the Easter Offensive] and January 1973 [the Paris Peace Accords following the Linebacker II bombings of North Vietnam] at the more modest level of "over 4,000.") In the First Gulf War, over 17,000 precision-guided weapons were expended over a period of roughly six weeks. Using the higher figure of 10,500 for the Vietnam War yields a rate of a little over 800 per month, or 200 a week. This compares to over 2,800 per week during the First Gulf War, for a ratio of 14:1. Barry D. Watts, *Six Decades of Guided Munitions and Battle Networks* (Washington, DC: Center for Strategic and Budgetary Assessments, 2007), p. 9; Headquarters, *Pacific Air Forces, Summary, Air Operations Southeast Asia*, monthly reports for May 1972 through January 1973 cited in Thomas A. Keaney and Eliot A. Cohen, *Gulf War Air Power Survey Report* (Washington, DC: U.S. Government Printing Office, 1993), p. 226. Moreover, the U.S. military did not fully embrace precision-guided weapons until after the First Gulf War.

recently seen the Chinese military test several types of anti-satellite (ASAT) weaponry.[16] Viewed from this perspective, cyber warfare joins "precision warfare" and a growing competition in space as the newest, and arguably the least understood, form of warfare.

Before proceeding further, a few definitions are in order. First, what is cyber space? For the purposes of this assessment, cyber space comprises all of the world's computer networks. Thus cyber space includes both open and closed networks and everything they connect and control, to include the computers themselves, the transactional networks that send data regarding financial transactions, and those networks comprising control systems that enable machines to interact with one another, such as Supervisory Control And Data Acquisition (SCADA) systems that regulate pumps, valves, elevators, generators, and other machines.[17]

Cyber warfare, then, can be defined as actions by nation-states and non-state actors employing cyber weapons to penetrate computers or networks for

16 Craig Covault, "Chinese Test Anti-Satellite Weapon," *Aviation Week and Space Technology*, January 17, 2007.

17 The definitions of cyber space and cyber warfare are drawn from Richard A. Clarke. See Clarke and Knake, *Cyber War*, p. 70.

the purpose of inserting, corrupting, and/or falsifying data; disrupting or damaging a computer or network device; or inflicting damage and/or disruption to computer control systems.[18] Cyber war can involve engaging in acts of espionage, criminal activities, and economic warfare. It can also include actions designed to support military operations at the tactical and operational levels of war, as well as independent operations designed to achieve strategic effects. While this report touches upon many of these operations, its principal focus is on independent cyber warfare operations whose intent is to achieve strategic effects (i.e., to produce catastrophic destruction in the state that is the target of cyber attacks).

Finally, what constitutes a catastrophic event? Webster's dictionary defines it as "a momentous tragic event ranging from extreme misfortune to utter overthrow or ruin." For our purposes we can interpret "utter overthrow or ruin" as the end of a regime or even the disintegration of a state or loss of its sovereignty. This is a high standard to meet. What of the more modest definition of the term: "extreme

18 Ibid., pp. 6, 228.

misfortune"? This criterion is far less daunting, in part because it leaves much open to interpretation. Perhaps this is why policy-makers seem so fond of warning of the potential for "catastrophic" destruction or consequences without providing any specifics. Like Supreme Court Justice Potter Stewart and pornography, it seems senior policy-makers cannot define "catastrophic destruction" but will "know it when they see it."

AIR POWER AND CATASTROPHIC DESTRUCTION

To some degree, the ongoing debate over the answer to the question of what constitutes catastrophic destruction recalls the debate over air power in its infancy. General Keith Alexander, the commander of U.S. Cyber Command, has stated, "The cyber domain in some ways is like the air domain, in being a realm that had no relevance for military planning until all of a sudden a new technology offered access to it."[19] At the risk of overdoing the analogy between the development of conflict in the air and cyber domains, one recalls that initially air forces

19 Keith B. Alexander, statement before the House Armed Services Committee, September 23, 2010, p. 4.

emphasized "extracting data" about their rival's forces through reconnaissance operations in the form of air patrols across "no man's land" on the Western Front in World War I. It did not take long before aircraft took on a more active role. Planes were fitted with machine guns both to keep enemy aircraft from invading friendly airspace to gather information as well as to protect them. Once armed, it was a short step to assigning aircraft to conduct attacks on enemy ground installations and forces. The competition evolved from merely "extracting data" to actively "corrupting" the enemy's systems, both military and industrial. Toward the end of the war both Britain and Germany took the first halting steps toward strategic aerial bombardment. The British established the Independent Air Force in the summer of 1918 that proceeded to bomb German installations and population centers beyond the front lines. Earlier in the war the Germans employed air ships and later Gotha bombers to drop bombs on London. The results of both these efforts were exceedingly modest.[20]

20 William R. Muscha, "Strategic Airpower Elements in Interwar German Air War Doctrine," U.S. Army Command and General Staff College, 2001, pp. 12-14, 23-25, 28, available at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA396938, accessed on February 29, 2012; and David T. Zabecki, *The German 1918 Offensives: A Case Study in the Operational Level of War* (New York: Routledge, 2006), p. 82.

A willingness to view civilians as combatants was central to this way of thinking, but far from unprecedented. There is a long history of combatants inflicting the costs of war on civilians, for example in the form of maritime blockade. Air forces were first employed while a blockade was being waged by Britain's Royal Navy against Germany during World War I. The blockade imposed severe hardships on the German people and contributed indirectly to the causes of the 1918 revolution that ended the reign of the Hohenzollerns.

Not long after the Great War ended, air power theorists began to assert that the potential existed for air forces, acting independently of ground and naval forces, to strike enemy forces and, even more importantly, to inflict through aerial bombardment prompt, catastrophic destruction on the society and industrial base that sustained the enemy's forces in the field. Among these air power enthusiasts was British Air Marshal Hugh Trenchard, who asserted:

> It is not necessary, for an air force, in order to defeat the enemy nation, to defeat its armed forces first. Airpower can dispense with that intermediate step....[21]

21 As quoted in Igor Primoratz, *Terror from the Sky: The Bombing of German Cities in World War II* (Oxford, United Kingdom: Berghahn Books, 2010), p. 23.

British Prime Minister Stanley Baldwin accepted Trenchard's argument, and declared that:

> Any town that is within reach of an aerodrome can be bombed within the first five minutes of war from the air . . . and the question will be whose morale will be shattered quickest by the preliminary bombing? I think it is well for the man in the street to realise that there is no power on earth that can protect him from being bombed. Whatever people may tell him, the bomber will always get through.[22]

Trenchard and Baldwin were echoing the views of the Italian Giulio Douhet, perhaps the leading air power theorist of the time. Douhet extended this line of thought one step further, declaring that "[T]he side which decides to go to war will unleash all its aerial forces in mass against the enemy nation the instant the decision is taken, without waiting to

22 Stanley Baldwin, "A Fear For the Future," *The London Times*, November 11, 1932, p. 7. Baldwin's concerns were well-founded in the sense that at the time of his observation early warning of a bomber attack was limited to visual and auditory detection. Radar had yet to be developed, and hence both defensive fighter aircraft and ground-based anti-aircraft units would have little warning that an attack was imminent. This situation made it difficult, if not impossible, for the defender to prevent a bomber force from reaching its target. Of course, things changed dramatically with the introduction of radar and the creation of integrated air defense systems, arguably the world's first "battle networks."

declare war formally."[23] In the wake of such an attack, Douhet went on to note

> A complete breakdown of the social structure cannot but take place in a country being subjected to . . . merciless pounding from the air. The time would soon come when, to put an end to horror and suffering, the people themselves, driven by the instinct of self-preservation, would rise up and demand an end to the war.[24]

Writing around the same time, the famous British military theorist Major General JFC Fuller concluded that should London be subjected to aerial bombardment by modern aircraft, it would be quickly reduced to chaos and its government "swept away by an avalanche of terror."[25]

Aviation enthusiasts proved long on vision but short on analysis. Despite major advances in aviation technology and capabilities in the decade or so that followed the writings of Douhet, Fuller, and others like the American aviator, Brigadier General

23 Joseph Patrick Harahan and Richard H. Kohn, eds., *The Command of the Air* (Tuscaloosa, AL: University of Alabama Press, 2009), p. 202.

24 Ibid., p. 58.

25 Paul Johnson, *Modern Times: The World from the Twenties to the Nineties* (New York: HarperCollins, 2001), p. 349.

Billy Mitchell, along with the dire predictions of men like Stanley Baldwin, when their theories and predictions were put to the test in World War II, strategic aerial bombardment failed to measure up. The predicted results did not materialize. Societies did not collapse. If anything, civil society proved remarkably resilient on both sides in the face of heavy bombing, the brunt of which fell not on the military, but on the people and the state's economic infrastructure.

This is not to say that air power did not play an important role in the war; it did. Moreover, despite the pessimistic conclusions of the U.S. and British Strategic Bombing Surveys undertaken after the war, later scholarship suggests that the air campaign produced important indirect, or second-order effects.[26] What did not occur was either prompt, catastrophic destruction or the kind of "extreme misfortune" that would cause a society to unravel and either collapse or turn on its government.

Put another way, the German "blitz" against Great Britain, the U.S. and British strategic bombing

26 See James G. Roche and Barry D. Watts, "Choosing Analytic Measures," *Journal of Strategic Studies*, June 1991, pp. 172-84.

campaign against Germany, and the U.S. strategic bombing campaign against Japan all failed to produce the direct collapse of the enemy's ability or will to persist in the conflict without the need to achieve victory in the traditional sense through a direct clash between armed forces. To the extent strategic bombing failed to destroy the enemy's ability to resist, it was left with the objective of causing the collapse of the enemy's will to persist. Thus the decision of whether or not to continue the war was ceded to the target of the strategic bombardment campaign. It would take another half century, until the first intense use of precision-guided munitions (PGMs) in the First Gulf War, for air power to produce anything close to the kind of effects envisioned by men like Douhet and Trenchard.[27]

The United States' introduction of nuclear weapons in 1945 radically changed the debate. Air power enthusiasts may have been wrong with respect to the ability of standard explosives to inflict prompt, catastrophic damage, but the same could not be said

27 For a treatment of the rise of guided weaponry, see Watts, *Six Decades of Guided Munitions and Battle Networks: Progress and Prospects*.

regarding a strategic bombing campaign employing aircraft equipped with nuclear weapons.

Two atomic attacks were made by the United States against Japan in the closing days of World War II. Nuclear weapons had an impact on warfare unlike any piece of military equipment that came before it, or that has emerged since.[28] In the period immediately following the introduction of nuclear weapons, however, the United States lacked sufficient numbers of them to bring about prompt, catastrophic destruction against a major nation-state, such as its emerging rival the Soviet Union. Thus while nuclear weapons gave both strategic aerial bombardment and the prospect of the rapid collapse of enemy resistance a rebirth, it was not until these weapons were available in large numbers and combined with the advent of fusion weapons (i.e., thermonuclear weapons, or the Hydrogen Bomb) of nearly limitless destructive power in the early 1950s that their promise was fully realized.

28 For an excellent discussion of the early period of the nuclear competition, see Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: St. Martin's Press, 1981), pp. 3-44.

THE SHOCK FACTOR

In addition to its destructive potential, some senior policy-makers, including Secretary of Defense Panetta, seem to attach importance to the shock that they believe could accompany a cyber attack that disabled major parts of a country's infrastructure; hence the reference to a cyber "Pearl Harbor."[29] While the attack on U.S. naval and air facilities on Hawaii in December 1941 did not produce catastrophic destruction, it was a terrible shock to the nation. In this case, the shock was quickly transformed into a steely national resolve among the American public that would be sustained over four years of war under difficult circumstances and at great cost until victory against Japan was achieved.

But what about the combination of prompt, catastrophic destruction delivered in such a manner as to provoke the kind of shock that accompanied the attack on Pearl Harbor or, more recently, the terrorist attacks on New York and Washington in September 2001? This issue was given serious consideration by senior Allied leaders with respect to the first use of

29 "CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor," *ABC News*, February 11, 2011, p. 2.

atomic weapons. Liddell Hart argued that when trying to break the will of an adversary:

> decisive results come sooner from sudden shocks than long-drawn-out pressure. Shocks throw the opponent off balance. [Gradual] pressure allows him time to adjust to it.[30]

Both Secretary of War Henry Stimson and Army Chief of Staff General George Marshall agreed. After Japan's defeat Stimson wrote: "I felt that to extract a genuine surrender from the Emperor and his military advisers they must be administered a tremendous shock which would carry convincing proof of our power to destroy the Empire."[31] Stimson recalled that General Marshall accorded "high value" to the weapon's potential to shock Japan's leaders. Marshall himself stated:

> It's no good warning them. If you warn them there's no surprise. And the only way to produce shock is surprise.[32]

30 B. H. Liddell Hart, *The Revolution in Warfare* (New Haven, CT: Yale University Press, 1932), p. 121.

31 Henry L. Stimson, "The Decision to Use the Atomic Bomb," *Harper's Magazine*, 194, No. 1161, February 1947, p. 101.

32 As quoted in Max Hastings, *Retribution: The Battle for Japan*, 1944-45 (New York: Random House, 2009), p. 476.

Viewed from this perspective an argument can be made that absent a level of destruction that, by itself, triggers "utter overthrow or ruin"—something that was not possible in 1945 with the handful of fission weapons available to the Americans—the ability to shock the target population may provide the difference between success and failure. In other words, it is possible that the level of destruction inflicted, combined with the manner in which it is inflicted, can produce catastrophic results. In the case of Hiroshima and Nagasaki, Japan still possessed the capability to pursue the war after the atomic attacks. Moreover, Japan had suffered even worse devastation from single bombing raids such as the one against Tokyo in March 1945.[33] The atomic attacks, however, represented an entirely new kind of warfare, certainly to the Japanese people as well as to most of its senior leadership. While the debate over whether the attacks were necessary to induce Japan's surrender goes on even today, those who argue the attacks were justified cite as partial evidence

33 On the night of March 9-10, 1945, over 200 U.S. B-29 bombers conducted an incendiary bombing raid on Tokyo, killing over 80,000 Japanese. Cited in Walter Russell Mead, *Special Providence* (New York: Routledge, 2002), p. 219.

the shock effect they had on Japan's leaders.[34] As one scholar noted:

> It was not that the military men had suddenly become reasonable in the hours following the Hiroshima and Nagasaki disasters; it was rather that they... had momentarily been caught off balance. They were also at a loss of words which could make any lasting impression upon the end-the-war faction. Prior to the dropping of the two A-bombs they had been able to pledge their belief in their ability to meet effectively any action taken by the enemy, but now whatever they said made them look foolish and insincere.[35]

This raises the possibility that, as in the case of the first nuclear attack, the success of the first cyber strike whose objective is to inflict catastrophic destruction could be, to a significant degree, a function of the target population's shock. That said, the "shock effect" is likely to be a singular event. As Lawrence Freedman notes with respect to the first use of nuclear weapons, "the advantage

34 Sadao Asada, "The Shock of the Atomic Bomb and Japan's Decision to Surrender—A Reconsideration," *Pacific Historical Review*, 67, No. 4, November 1998, pp. 477-512.

35 Robert C. J. Butow, *Japan's Decision to Surrender* (Stanford, CA: Stanford University Press, 1954), p. 180, cited in Freedman, *The Evolution of Nuclear Strategy*, p. 20.

of shock was unique; thereafter there could be horror but not surprise in the bomb's use."[36] Moreover, the production of large numbers of nuclear weapons over the next decade or so by both the United States and the Soviet Union left little doubt that the "shock effect" of a nuclear attack would not be necessary to inflict catastrophic consequences on the targeted society.

It may be, therefore, that for cyber warfare the first attack designed to inflict catastrophic destruction will be aided significantly by the shock effect of such an attack. If that proves to be the case, then, as with nuclear weapons, the effect is likely to be ephemeral. Subsequent attacks will not likely enjoy the benefit of such a shock effect. If today cyber weapons must rely on shock to generate catastrophic results, like their nuclear predecessors they will either need to become more numerous

36 Freedman, *The Evolution of Nuclear Strategy*, p. 20.

and/or powerful, or they will lose the ability to inflict catastrophic destruction.[37]

PROMPTNESS AND COST IMPOSITION

Promptness

There is also the matter of what is meant by "prompt" effects. In the Cold War era context of a massive nuclear exchange between the United States and the Soviet Union, the effects would be almost instantaneous. While cyber attacks can be executed at the speed of light, the effects generated from such attacks may not be felt for days, weeks, or perhaps even several months. The longer the effects of such an attack take to play out, the less the attacker would appear to be relying on shock effect and more on the damage caused by the attack. To be sure, the effects

37 The value of any shock effect can be further diminished by other factors. In the case of Japan in August 1945, Freedman notes that the atomic attacks induced a measure of shock, but that Japan was already on the verge of collapse. Thus the shock effect was akin to "administering poison on the death bed." Freedman, *The Evolution of Nuclear Strategy*, p. 20. It should also be noted that the shock of an attack can induce resolve rather than resignation in the target. A classic example, of course, is the American reaction to the Japanese attack on Pearl Harbor. While shocked, the Americans had the means to fight back, and they did with a vengeance. A similar reaction occurred with Germany's aerial bombardment of Great Britain in 1940-41, known as the "Blitz." Far from breaking British resolve, the bombing strengthened it. Finally, despite the predictions of some that Iraq would quickly collapse in 2003 from "shock and awe" in the wake of a massive U.S. precision-strike aerial bombardment, it failed to occur, even though Iraq did not have the means to pose any significant threat to the United States. This would serve to make Freedman's point regarding the diminishing value of "shock" once a new form of warfare (in this case, strategic precision bombardment) is employed. Yet there is little evidence that Iraqi leaders were shocked even when precision-guided weapons were employed by the U.S. Air Force against Iraq in the First Gulf War in 1991. The phrase "shock and awe" is taken from Harlan K. Ullman and James P. Wade, *Shock and Awe : Achieving Rapid Dominance* (Washington, DC: National Defense University, 1996).

could be catastrophic, but more along the lines of the accumulated effect the Royal Navy's blockade had on Germany during World War I. If this proves to be so—i.e., if it turns out that a cyber strike can inflict catastrophic damage, but only after the passing of an extended period of time, say many months—then it seems likely that other forms of military power will also be brought to bear in the conflict. In these circumstances it may be difficult to determine whether cyber weapons, by themselves, produced catastrophic damage.

Cost Imposition

There is one final issue worthy of consideration when exploring the possibility of cyber weapons inflicting catastrophic damage. It pertains to long-term cost imposition. In this case the level of damage would not need be extensive, certainly nothing compared to the damage inflicted by a major nuclear attack or even that of a major air campaign employing precision-guided weapons. Nor would the effects have to be prompt, occurring within a few hours, days, or even weeks.

Consider a major attack conducted along relatively compressed timelines (again, we are talking a matter of days, not weeks) that inflicts catastrophic damage of a milder sort—damage amounting to "extreme misfortune" of the targeted state rather than damage that results in its "utter overthrow or ruin." Cost imposition might be considered a catastrophic effect in the context of "extreme misfortune" if it results in the targeted society being forced to undertake a major and perhaps even a fundamental shift in the way it is organized and functions such that it incurs enormous and sustained costs over time.

For example, if a series of cyber attacks produced repeated power blackouts in an area over a protracted period of time, there would likely be a loss of confidence in the electric utilities' ability to provide reliable power to businesses and homes. While people are generally prepared to deal with the occasional brief power outage that lasts a few minutes or so, and the rare extended outage (e.g., following a major storm) every few years, none are prepared for frequent outages lasting many hours or even several days. Were this to become common, it

seems likely that those businesses and homeowners who could afford to have backup power (e.g., generators, solar-powered batteries, etc.) would invest in it. The costs of permanently shifting to this new way of life would be substantial and enduring. To the extent that similar problems could arise in areas like other utilities (e.g., gas, water transportation, and finance), the cumulative costs could be both enormous and persistent. The consequences would be catastrophic in the sense that the targeted country would have suffered "extreme misfortune."

For this kind of large-scale cost imposition to occur, the mode of attack and the defenses arrayed against it would have to favor the offense, such that the long-term costs of conducting attacks would be far less than those required to mount an effective defense against them. The classic example of this, of course, is the nuclear competition. Here the balance between offense and defense has been heavily weighted toward the offense, and has remained so in the sixty-seven years since nuclear weapons were introduced. Thus we can say that in the nuclear case the balance is both offense-dominant and stable

(i.e., it has consistently favored the offense and shows no indications of changing any time soon). Indeed, in the case of nuclear weapons delivered by ballistic missiles, no effective defense has yet to emerge at any plausible cost. To paraphrase Stanley Baldwin: The missiles (or enough of them) will always get through.

The questions with respect to cyber warfare as it pertains to catastrophic destruction are: Is the competition offense-dominant? Is the competition stable or dynamic?

Taking the foregoing discussion into account, for the purposes of this paper the term "catastrophic" implies, at the high end, the imposition of costs such that the target is no longer willing or capable of resisting the political will of the attacker, and at a minimum that the target incurs major long-term (i.e., enduring and recurring) costs—economic, social, and political—that are far in excess of those incurred by the attacker to generate his attack. This definition is particularly relevant with respect to non-state entities whose sole purpose may be to inflict pain and not to realize any well-defined political objective. As suggested above, the term "prompt" does not mean

“instantaneous” (as, for example, it has come to be associated with a massive nuclear attack), but rather occurring over a relatively extended period of time, perhaps many months, although less than years.

We now turn to a discussion of the issue of cyber warfare and the potential of cyber attacks to create prompt, catastrophic destruction.

CHAPTER 3 > **BACKGROUND TO THE CURRENT SITUATION**

The threats to U.S. national security in the 21st century are numerous. As alluded to by U.S. leaders and others, arguably the newest formidable threat, the one with the lowest barriers to entry to those who wish to pose it, is cyber warfare. Its potential to inflict serious and perhaps catastrophic damage on critical infrastructure, to include the power, energy, and financial sectors, has attracted growing attention from both the public and private sectors of nearly every state with an advanced information technology (IT) infrastructure.

While cyber warfare may seem "new," it has been a part of the geostrategic landscape for at least 15 years, and perhaps as long as 30. It is not clear when nation

states began to engage in significant cyber activity. There are reports that in 1982 President Ronald Reagan approved the covert introduction of malware into a supervisory control and data acquisition (SCADA) system that resulted in a large-scale explosion and major damage to a Soviet gas pipeline.[38]

As the Internet experienced its rapid expansion in the 1990s, hackers began engaging in cyber "pranks" while low-level criminals began exploring the potential for cyber crime. Once it was shown that "crime pays" in the cyber domain, organized crime began muscling its way onto the scene, in some cases apparently with the blessing—and even support—of the governments on whose territory they were operating.[39]

What follows is a *partial* summary of some of the more significant *known* cyber operations. As cyber operations are typically shrouded in secrecy, and as victims of cyber operations are often reluctant to advertise their vulnerability, this summary is not intended to be comprehensive, but illustrative. The objective is to give the reader a sense of the trends in cyber operations so as to provide an understanding

38 John Markoff, "Old Trick Threatens the Newest Weapons," *New York Times*, October 26, 2009.

39 Gus W. Weiss, "The Farewell Dossier: Duping the Soviets", *CIA Studies in Intelligence*, 39, No. 5, 1996

of where the cyber competition stands today and what these trends might tell us about the future, particularly cyber weapons' potential for triggering catastrophic effects.

THE EARLY YEARS

With the rise of cyber commerce in the late 1990s, cyber criminals arrived on the scene. Some of the earliest and likely most effective cyber criminal operations were conducted through distributed denial-of-service (DDoS) attacks. This was followed by widespread efforts at identity theft. During this period cyber crime began serving as a kind of laboratory where malicious payloads and exploits used in cyber warfare could be developed, tested, and refined.

A DDoS attack occurs when many malicious hosts coordinate to flood the target network with large amounts of traffic simultaneously. The attack's objective is to deny service by exhausting the target's resources. These resources can be network bandwidth, computing power, or operating system data structures. To launch a DDoS attack, malicious

users first build a network of computers that they will use to produce the volume of traffic needed to deny services to computer users. To create this attack network, attackers discover vulnerable sites or hosts on the network.[40] As the attacker gains access to vulnerable systems, he installs programs or "attack tools," converting the system into a "bot" or "zombie" that can now be remotely controlled by the attacker. Masses of bots or zombies are called "botnets" or cyber "armies." Since the process for scanning for vulnerable computers can be automated, botnets can be created relatively quickly.

Unlike malicious hackers, criminals engaging in cyber crime were (and are) not interested in using viruses to delete files, turn machines off, or even broadcast love for a stripper (as the Melissa virus did). Rather, cyber criminals were seeking to take

40 Vulnerable hosts typically are those with no antivirus software or out-of-date antivirus software. Identifying these kinds of computers and installing attack tools on them has become a relatively easy, automated process. Attack tools are available in the form of prepared programs that, "automatically find vulnerable systems, break into these systems, and then install the necessary programs for the attack. After that, the systems that have been infected by the malicious code look for other vulnerable computers and install on them the same malicious code. Because of that widespread scanning to identify victim systems, it is possible that large attack networks can be built very quickly." This process creates a botnet comprising a controller (handler or master) who can now exercise control over a large number of "zombie" computer systems that can be coordinated to conduct massive simultaneous attacks against a given target. The above discussion of DDoS attacks is summarized from Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki, "Distributed Denial of Service Attacks," *The Internet Protocol Journal*, 7, No. 4, available at http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html, accessed on January 20, 2012.

control of computer systems and use them to send email (i.e., spam), enabling DDoS attacks. Such attacks have been used, for example, to extort payment from gambling websites by threatening to take them off-line during periods of peak business (e.g., immediately prior to major sporting events like the Super Bowl).[41]

The Love Bug

While potential major problems associated with computer systems and networks were hardly unknown in the 1990s (e.g., the Y2K scare),[42] arguably it was not until 2000 that the power of computer viruses was revealed. That year the Love Bug virus was set loose by a pair of hackers in the Philippines. The virus successfully attacked roughly 55 million computers.[43] The malware was sent to a com-

41 Andress et al., *Cyber Warfare*, p. 176. See also Menn, *Fatal System Error*, pp. 5-11. Menn describes an early DDoS attack against a gambling site in which the site's owners were puzzled by their site's sluggish web page. Large numbers of computers were contacting the web site, but failed to place bets. The owners soon received an email from the attacker explaining that they were the victims of a DDoS attack, along with an extortion demand.

42 Richard Lacayo, "The End of the World As We Know It?," *Time Magazine*, January 18, 1999. The Y2K scare resulted from concerns emanating from the programmer practice of abbreviating year designations from four digits to two (i.e., 1999 becomes "XX99"). The concern arose over what would occur when the year 2000 arrived: would computers believe they had been reset to the year 1900, or not? Or would they simply malfunction? Apparently most businesses patched their systems and successfully avoided the problem.

43 Kevin Poulsen, "Tained 'Love' Infects Computers," *Wired*, May 3, 2010, available at http://www.wired.com/thisdayintech/tag/love-bug/, accessed on January 10, 2012.

puter user as an attachment to an email with the text "ILOVEYOU" in the subject line. If the recipient opened the attachment, the worm embedded in it sent a copy of itself to everyone in the user's address book. The worm also made a number of malicious changes to the user's system, overwriting files with a copy of itself.[44] Only computers with the Microsoft Windows operating system were vulnerable. However, reflecting the risks associated with a largely global computing monoculture, estimates of the damage wrought by the Love Bug ran as high as $15 billion.[45]

SoBig, Bagle, and My Doom

In 2003, a virus far more threatening than the Love Bug arrived on the cyber scene. The initial version, named SoBig, spread by persuading recipients to open a mislabeled attachment containing a malicious program. Once activated, like the Love Bug, the SoBig virus looked for new addresses to whom

44 The virus could also have been employed to create zombies for a botnet.

45 Joseph S. Nye, Jr., "Power and National Security in Cyberspace," in Kristin M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age* (Washington, DC: Center for a New American Security, 2011), p. 13.

it could mail itself. What made SoBig different was that it instructed infected machines "to check in with other computers, whose location would be revealed only at the last instant, to get additional cyber tools and instructions."[46]

In other words, all of the infected machines had the potential to be employed as zombies in a botnet. The creators of SoBig could therefore use an email program to communicate with these zombies, and instruct the machines to generate millions of messages (e.g., as part of a DDoS attack, or a phishing[47] campaign) while also disguising the initial source of the mailing, making it difficult to identify the true source of the attacks.

Shortly thereafter enhanced versions of SoBig began spreading. Each new version—named SoBig.B, SoBig.D, etc.—was more sophisticated than the last, to include correcting bugs found in

46 Menn, *Fatal System Error*, p. 103.

47 Phishing involves sending spam disguised as legitimate emails to trick people into revealing personal information, such as their social security numbers, bank account numbers and passwords, and other information that could be used for financial gain. It may also involve attempts to trick the recipient into revealing other kinds of information, such as passwords to access computer networks that could be used for the purpose of espionage, planting logic bombs, or other illegal or aggressive activities. Literally millions of messages are sent in the hope of inducing a very small percentage of people to open them and compromise themselves. Botnets are particularly useful in conducting phishing campaigns. Menn, *Fatal System Error*, p. 113; and Edward Skoudis, "Information Security Issues in Cyberspace," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009), p. 175.

earlier versions. Mysteriously, after spreading for two weeks, the worm was programmed to turn itself off. This led to suspicion that SoBig may have been some kind of cyber weapons field test, or "proof-of-principle" exercise.[48]

SoBig proved challenging for both law enforcement agents and commercial cyber security professionals. It took six months for cyber security experts to identify and evaluate the code underlying SoBig, to include the changes made to each successive version. They concluded that the program's "fingerprints" or "stylistic tics" matched those of a Russian company that made software called Send-Safe, one of the world's leading providers of spamming services.[49]

SoBig was followed by Bagle and MyDoom. Both are suspected of being the first truly "commercial" viruses.[50] Once Bagle penetrated a computer or computer network, it opened a trap door enabling later downloads through the opening. In so doing, it turned the captured computers into open relays for spam generation. Similarly, MyDoom employed

48 Menn, *Fatal System Error*, p. 103.

49 Ibid., p. 107.

50 Ibid., p. 105.

a Trojan horse, infecting millions of computers and then opening a secret backdoor for its author, who could then use these computers as a botnet to conduct denial-of-service attacks or generate large amounts of spam for phishing operations.[51]

What proved perhaps most interesting about the MyDoom virus was that in February 2004 the latest version included a copy of its source code. (In July, a new Bagle release did the same.) The widespread availability of high-end virus code meant that any individual with modest cyber hacker skills could take and modify these source codes and, in so doing, potentially take control of large numbers of computers; hence the "commercial" appellation. Some cyber security experts were puzzled as to why the viruses' authors would share their code and empower potential competitors. Speculation arose that the authors were protecting themselves in the event that the original code was found stored on their computers. If the same or very similar code were on

51 MyDoom caused an estimated $4.8 billion in damage, the second-most-expensive software attack ever up to that time. "Hacker Hunters," *Bloomberg Business Week*, May 30, 2005, available at http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm, accessed on March 3, 2012.

tens of thousands of machines, then the otherwise critical evidence against them would be worthless.[52]

Estimates of the damage from the three giant spam-driven viruses ran well into the billions of dollars. Despite the damage done, no criminal charges were ever brought against the authors of SoBig, Bagle, and MyDoom, which strongly suggests that crime does indeed pay, and that in the competition to protect computer systems, the balance was heavily weighted toward the offense when it came to penetrating individual user machines.

The Rise of Botnets

Despite the work of talented hackers and cyber criminals noted immediately above, a German teenager, Axel Gembe (also known as "Ago"), may have done more than anyone else to put botnets in the mainstream of cyber crime and, perhaps, cyber war. Gembe attended school in a small Black Forest village in Germany, dropping out in the ninth grade. A self-taught programmer, Gembe developed a worm that he called Agobot. Agobot's claim to fame was

52 Menn, *Fatal System Error*, p. 111.

its adaptability. Anyone with Agotbot's source code could add new exploits to it as they became available, enabling it to be constantly improved. Agobot was used by Lee Walker, a British citizen helping Paul Ashley, an American, develop the capability to conduct denial-of-service attacks for a client. Walker provided the Agobot code, expertise, and botnets that enabled Ashley to cripple the websites of his client's competitors.[53]

Walker's ability to take Gembe's worm and apply it for his own particular purpose was a major factor in bringing "DDoS-for-hire" services into the cyber marketplace.[54] For Russian groups like Send-Safe and others who sent billions of pieces of spam, the proliferation of competitors hawking their botnets drove down profits, but it hardly drove them out of business. Criminals possessing virus-controlled botnets continue to generate huge amounts of spam,[55] offering their services to the

53 Ibid., p. 112.

54 Ibid.

55 It is estimated that most of the Internet's email traffic is comprised of spam, perhaps as much as 80 percent. Larry Barrett, "Worldwide Spam Traffic Falls to 2-Year-Low," *eSecurity Planet*, January 26, 2011, available at http://www.esecurityplanet.com/trends/article.php/3922271/Worldwide-Spam-Traffic-Falls-to-2Year-Low.htm, accessed on January 10, 2012.

highest bidders, with the Russians remaining the worst offenders.

As profits declined from DDoS services, criminal groups began using botnets for identity theft primarily through phishing attacks. Today cyber criminals, primarily Eastern European organized crime groups, purportedly possess about half of the world's credit card numbers, according to the head of the U.S. Justice Department's computer crime section.[56]

It is estimated that as recently as 2009 that some 1,000 botnets, or "zombie armies," of considerable size exist, with another 100 or so more sophisticated botnets directed with greater stealth.[57] Finally, it is believed that there may be a handful, perhaps 10 or so, of botnets controlled in a manner similar to the recent Conficker worm (see below) in peer-to-peer fashion, with computer "drones" updating each other.[58] In the current environment, it may be that absent the centralization of computing power (perhaps

56 Menn, *Fatal System Error*, p. 210.

57 Ibid., pp. 230-231.

58 Ibid., p. 231.

through a mechanism like the Cloud)[59] that can be made secure from attack, there may be no way to overcome the threat posed by these botnets.

CYBER CRIME AND THE STATE

Organized crime has been a major catalyst in the expansion of illicit cyber activity. Nowhere has this been more apparent than in Russia, where the Russian Business Network (RBN) has emerged as "the world's foremost cyber-crime organisation, as a provider of the logistic basis for cyber attacks."[60] The RBN's cyber warfare capabilities are so formidable that it is the only criminal organization that has been identified by NATO as a major security threat.[61] It has conducted attacks in part through its botnet armies. Its largest (and the world's largest) botnet army, known as *Storm*, has

59 Phil Stewart, Diane Bartz, Jim Wolf, and Jeff Mason, "Special Report: Government in Cyber Fight But Can't Keep Up," *Reuters*, June 16, 2011, p. 1. Cloud computing provides computing in the form of a service rather than as a product. For example, instead of purchasing and installing a piece of software on a personal computer, the computer accesses the software from a remote location (in the "Cloud") as a service. This service is provided on a metered basis over a network, such as the Internet. See "Cloud computing," Wikipedia, available at http://en.wikipedia.org/wiki/Cloud_computing, accessed on January 21, 2012.

60 Alexander Klimburg, "Mobilising Cyber Power," *Survival*, 53, 2011, p. 49 as referenced in "A Walk on the Dark Side," *The Economist*, 2007, available at http://www.economist.com/nodc/972376, accessed on June 1, 2012.

61 Klimburg, "Mobilising Cyber Power," *Survival*, p. 49.

reportedly provided approximately one-fifth of the world's spam email, selling this service and others to anyone with the money to rent them, from other cyber criminals to hacktivists to cyber "patriots."[62] The RBN is thought to control between 150 and 180 million nodes.[63] In 2007 roughly 40 percent of global cyber crime, which some estimate exceeded $100 billion at that time, was attributed to RBN.[64]

The Russian government is aware of the RBN's activities. Rather than working to suppress it, however, it appears Moscow turns a blind eye to the RBN's activities and may even rely on the RBN and other Russian cyber crime organizations as a sort of national cyber militia. Russian security services are known to recruit hacker patriots. The Nashi and Young Guard youth groups, created by President Vladimir Putin's ideological chief Vladislav Surkov, have been active in recruiting hackers for their cause. It is easy to imagine a cyber hacker being employed by RBN while in his spare time engaging in "patriotic"

62 Ibid., pp. 49-50.

63 Kevin Coleman, "Russia Now 3 and 0 in Cyber Warfare," *Defense Tech*, January 30, 2009, available at http://defensetech.org/2009/01/30/russia-now-3-and-0-in-cyber-warfare/#ixzz1isnC4rzP, accessed on January 10, 2012.

64 Klimburg, "Mobilising Cyber Power," p. 49.

cyber criminal activities as well. "Message boards and chat rooms located on Russian websites served as a meeting place for attackers, a place to coordinate their time of attack, discuss targets, and recruit others."[65] The RBN has also been accused of facilitating the attacks on Estonia in 2007 and Georgia in 2008, and of acting at the request (or direction) of the Russian government.[66]

One of the earliest cases of large-scale cyber espionage involving the Russian government and the country's cyber criminal element (i.e., RBN) occurred in the late 1990s. Known as Moonlight Maze, the operation saw large amounts of sensitive information stolen from the U.S. Defense Department, Energy Department, and National Aeronautics and Space Administration (NASA), as well as from some private firms.[67]

65 Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," *Culture Mandala*, 8, October 2008, p. 59.

66 Klimburg, "Mobilising Cyber Power," p. 50; and Clarke and Knake, *Cyber War*, p. 15.

67 Klimburg, "Mobilising Cyber Power," pp. 48-49.

RUSSIA AND THE FORMER EMPIRE

Estonia 2007

The 2007 cyber attacks on Estonia were precipitated by the Estonian government's decision to relocate a war memorial dedicated to the Soviet forces that liberated Estonia from the Germans during World War II. The statue was moved from a prominent position in Tallinn. The action triggered an angry response from the Russian government that was soon followed by DDoS attacks against Estonia's government and financial system, as well as on other targets. Moscow disavowed any knowledge of or responsibility for the attacks; however, Russian blogs contained instructions for how to join in the DDoS campaign.[68] Moreover, forensics traced some DDoS packets to Internet addresses within the Russian government. In its defense, a Russian government spokesman pointed out that the IP addresses could have been faked or the machines hijacked.[69]

Perhaps most interesting, the major part of the assault suddenly stopped roughly a month after it

68 Menn, *Fatal System Error*, p. 213.

69 Ibid.

began, suggesting that a botnet had been leased for the attacks. One Estonian official concluded that the attacks represented "a new form of public-private partnership" in which the attacks were executed by organized crime but directed by the Kremlin.[70] "In Estonia," said U.S. National Security Agency chief General Keith Alexander, "all of a sudden we went from cybercrime to cyberwarfare."[71]

Some experts believe the Estonia attack provided a way for Moscow to test cyber weaponry—a "proof of concept" in which the RBN was given a target to show the Russian authorities how valuable it could be.[72] In this way the attacks on Estonia might be viewed as roughly analogous to how the Spanish Civil War provided a testing ground for German, Italian, and Soviet equipment and war-fighting concepts. While the evidence is circumstantial, it appears that just as Germany used its military's experience in Spain to assist in its development of the blitzkrieg form of warfare it employed against Poland, the Low Countries, and

70 Ibid.

71 Ibid.

72 Ibid.

France shortly thereafter, the Russians used the lessons learned from their experience with Estonia to better integrate cyber operations with traditional military operations in Georgia.

Georgia 2008

A year later, in August 2008, Russian troops invaded Georgia following that country's launching of a military offensive against South Ossetia to reclaim territory from its Russian-backed government.[73] The offensive followed Georgian claims that its peacekeeping forces in South Ossetia were being attacked, and that Russia was deploying combat units into that country. Russia reacted by launching a counter-offensive in South Ossetia and against Georgia itself. Russian forces received support from separatist forces in South Ossetia and Abkhazia.

The Russian attacks were accompanied by denial-of-service network attacks. One series of cyber attacks shut down official sites in the Georgian city of Gori, along with local news sites, just prior

73 The 1991-92 South Ossetia War occurred shortly after the Soviet Union's collapse. The war ended with roughly half of South Ossetia under the control of a government that, while not enjoying recognition by the international community, did have Moscow's backing.

to Russian air strikes.[74] This led to claims that the attacks (which Moscow disavowed knowledge of) must have been coordinated with the Russian government. As in the case of Estonia, Georgian cyber security officials discovered that many of the attacks could be traced to servers controlled by the RBN.[75] It can be inferred, though hardly proven, that the Kremlin was sufficiently satisfied with the effects of the cyber attacks on Estonia as well as its degree of plausible deniability that it felt comfortable incorporating them into its war plans for Georgia.

The conflict was short-lived. Russian forces quickly gained the initiative and a cease-fire was agreed to on August 12, 2008. Two weeks later Russia recognized Abkhazia and South Ossetia as independent states.[76]

The Russian attack on Georgia appears to have been the first time cyber weapons were integrated at the operational level of war.[77] Just as radio and radar were integrated into operations during World War II to enhance the effectiveness of military forces,

74 Ibid., p. 214.

75 Ibid., p. 215.

76 As of 2011, only six states have recognized Abkhazia's independence, while only five have recognized South Ossetia.

77 The operational level of war is the level at which military campaigns are conducted to support an overall effort to accomplish strategic objectives.

cyber weapons appear to have been employed by the Russians to enhance their forces' effectiveness.

Kyrgyzstan 2009

Only five months after the conflict between Russia and Georgia ended, a third series of major cyber attacks occurred against the government and infrastructure of a former Soviet republic. On January 18th, 2009, Kyrgyzstan's two main Internet servers came under DDoS attacks.[78] The attacks were sufficiently strong as to shut down websites and email within the country.

The IP traffic was traced back to Russian-based servers known for cyber crime activity. The attacks occurred on the same day that the Russian government was pressuring Kyrgyzstan to terminate U.S. access to the airbase at Manas, a key logistics center supporting U.S. military operations in Afghanistan.[79] The cyber assault appeared to serve its purpose: Kyrgyzstan informed the United States

78 Dan Goodin, "DDoS attack boots Kyrgyzstan from net," *The Register*, January 28, 2009, available at http://www.theregister.co.uk/2009/01/28/kyrgyzstan_knocked_offline/, accessed on January 10, 2012.

79 Don Jackson, "Kyrgyzstan Under DDoS Attack From Russia," *Dell Secure Works*, January 27, 2009, available at http://www.secureworks.com/research/blog/research/20957/, accessed on January 10, 2012.

that its access to the Manas air base would be terminated. The attacks ceased shortly thereafter.

Russia's use of cyber warfare (if, indeed, Moscow authorized or directed the attacks) demonstrates the potential of cyber weapons to coerce states (as in the case of Kyrgyzstan) or to support military operations (as in the case of Georgia). In neither of these cases, however, nor in the case of Estonia, did the attacks produce anything remotely close to catastrophic destruction. To return to our air power analogy, they might be compared to the air operations conducted by the Condor Legion during the Spanish Civil War.[80]

CHINA

Background

China has also emerged as a major cyber power as measured by its involvement in cyber espionage and cyber crime. It is no exaggeration to say that China is waging economic warfare against the states

80 The Condor Legion comprised German "volunteers" operating German military aircraft in support of Spanish Nationalist forces during the Spanish Civil War, fought from 1936-39. The unit provided air support for Nationalist forces and engaged in acts of coercion and terror (e.g., the bombing of Guernica). While the Condor Legion did not play a decisive role in the conflict, it did provide a "proof of principle" for the role air power might play in both combined arms mechanized operations (i.e., blitzkrieg) and in strategic bombardment. See James Corum, "The Luftwaffe's Army Support Doctrine, 1918-1941," *The Journal of Military History*, 59, No. 1, January 1995, p. 67.

of the developed world in general, and the United States in particular. Hans Elmar Remberg, Vice President of the German Office for the Protection of the Constitution (Germany's domestic intelligence agency), describes the state of affairs well in noting that "across the world the [People's Republic of China] is intensively gathering political, military, corporate-strategic and scientific information in order to bridge their technological gaps as quickly as possible."[81] Cataloguing adversary weaknesses not only provides Beijing with an asymmetric advantage in the event of a conflict, it may also deter to cyber attacks by others, assuming accurate attribution is accomplished in the wake of such attacks. Moreover, if it can pose a credible threat to U.S. infrastructure or to the U.S. military's battle networks and information systems, China's cyber power may also enable it to buy time while it attempts to catch up to the United States in economic power and close the gap in traditional forms of military power. In any event, the People's Liberation Army's (PLA's) cyber warfare doctrine calls for China to achieve global

81 Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness", p. 57.

"electronic dominance" by 2050, enabling China to target its enemies' financial markets, military and civilian communications capabilities, and critical infrastructure with cyber strikes before traditional military operations begin—in effect executing a "cyber Pearl Harbor."[82]

China, with the world's largest Internet population, is also potentially highly vulnerable to cyber attack, as it has the most targets to defend. Its vulnerability is accentuated by the fact that it has a large number of computers operating with pirated Microsoft software, which do not receive and incorporate the latest security patch updates.[83] These factors, combined with the communist regime's concerns over internal dissent, find the Chinese government taking cyber defense very seriously.[84] For example, unlike the United States, all the networks that comprise China's Internet are controlled by the government, either through direct ownership

82 Mike McConnell, "Cyber Insecurities: The 21st Century Threatscape," in Lord and Sharp, eds., *America's Cyber Future: Security and Prosperity In the Information Age*, p. 30.

83 Fritz, "How China Will Use Cyber Warfare," p. 54.

84 The bulk of Chinese cyber activity is directed at supporting its police forces' efforts to suppress internal opposition groups. These efforts include propaganda and censorship, as well as attacks on web sites critical of the government or those associated with opposition groups. Klimburg, "Mobilising Cyber Power," p. 48.

or partnership with the private sector.[85] Unlike the U.S. government, Beijing has both the authority and the means to disconnect China's Internet from all external portions of the Internet, in effect instantaneously making China's national Internet more like a private corporation's intranet. In the event that China undertakes a massive cyber strike, the ability to "disconnect" itself from the global Internet could potentially reduce significantly its opponents' ability to retaliate and inflict comparable damage on China in a cyber counterstrike.[86]

Moreover, China has taken steps to address a key aspect of the monoculture problem when it comes to cyber defense. The Chinese State Planning Commission alleged that Microsoft's Windows operating system was one of the United States' secret cyber warfare weapons.[87] Consequently as a precondition to its doing business in China, Microsoft was required to provide the Chinese government with

85 Clarke et al., *Cyber War*, p. 146.

86 To be sure, there are other means besides the Internet for penetrating an adversary's computer networks, to include compromising their supply chain and the use of insiders with access to the network. These means are elaborated upon later in this report.

87 Gerald Posner, "China's Secret Cyberterrorism," *The Daily Beast*, January 12, 2010, p. 2, available at http://www.thedailybeast.com/articles/2010/01/13/chinas-secret-cyber-terrorism.html, accessed on January 20, 2012.

the source code for Microsoft Office software.[88] When Microsoft agreed to these terms, it effectively provided China with "skeleton keys" to its operating system, giving China a significant competitive advantage in infiltrating foreign computer systems and networks and in crafting advanced exploits.[89] Finally, unlike the situation in the United States, in China the PLA is responsible for both cyber offensive *and* defensive operations and for their entire nation, to include both government domains and the nation's critical infrastructure.[90] To the extent that the fundamental military maxim emphasizing "unity of command" has value in cyber warfare, this

88 It should be noted that the Chinese government is not the only government to have received elements of Microsoft's source code as a condition for doing business.

89 Posner, "China's Secret Cyberterrorism," p. 2; and Fritz, "How China Will Use Cyber Warfare," p. 67. Microsoft provided both China and Russia access to its source code in 2003 and 2002, respectively, and to both again in 2010. In the latter case, Microsoft provided Microsoft Windows Server 2008 R2, Microsoft Office 2010, and Microsoft SQL Server source code. Having access to the source code used in a monoculture could enable a government to identify weaknesses in the code that could be used to launch attacks. It is also possible to identify software vulnerabilities without having access to the source code. Identifying flaws in the code would also enable a state to patch those flaws in its own system to better defend itself. States engaged in such activities would have little incentive to inform the code's originator (Microsoft, in this case) as it would lose a potentially major source of competitive advantage. Tom Espiner, "Microsoft Opens Source Code to Russian Secret Service," *ZDNet*, July 8, 2010, available at http://www.zdnet.co.uk/news/security/2010/07/08/microsoft-opens-source-code-to-russian-secret-service-40089481/?tag=content;siu-container, accessed on March 3, 2012; Danko Danchev, "Does Microsoft's sharing of source code with China and Russia pose a security risk?" *ZDNet*, July 10, 2010, available at http://www.zdnet.com/blog/security/does-microsofts-sharing-of-source-code-with-china-and-russia-pose-a-security-risk/6789, accessed on March 3, 2012; and Charles Arthur, "Where, how and why would China get the source code to Microsoft's Windows?" *The Guardian*, December 4, 2010, available at http://www.guardian.co.uk/technology/2010/dec/04/microsoft-source-code-theft, accessed on April 19, 2012.

90 Clarke et al., *Cyber War*, p. 146. Cyber Command is responsible only for offensive and defensive cyber operations for the U.S. military.

may confer a major advantage on China in any cyber competition with the United States.

Views on Cyber War

China's military views its cyber operations as central to its competition with the United States. This view also appears to be highly consistent with Chinese strategic culture. The greatest of all Chinese strategic thinkers, Sun Tzu, observed, "all war is deception." The ongoing economic war that China is waging against the United States is masked by its government's repeated denials that such a war is even occurring, let alone on a massive scale. Success in its economic war with the West could help China over time surpass the United States as an economic power, and in so doing shift the military balance to the point where it could fulfill Sun Tzu's description of the greatest military leader as the one who can "win victory without fighting."[91]

As in the United States, there is discussion in Chinese professional circles regarding cyber weapons' potential to deliver prompt, catastrophic strikes

91 Timothy Thomas, "Google Confronts China's 'Three Warfares,'" *Parameters*, Summer 2010, p. 108.

against an enemy's critical infrastructure. For example, a 2008 analysis of PLA information security architecture requirements by a researcher at the Second Artillery College of Engineering in Xian noted that:

> electronic warfare [EW] and computer network warfare [or computer network attack—CNA] are the two primary modes of attack in information warfare . . . By using a combination of electronic warfare and computer network warfare, i.e., 'integrated network and electronic warfare,' *enemy information systems can be totally destroyed or paralyzed*.[92]

The following year, in a vein similar to that of the early air power theorists, Senior Colonel Wang Wei, a professor at the Nanjing Military Academy's Information Warfare and Command Department's Military Theory Teaching and Research Office, and Major Yang Zhen, a lecturer at the same office, argued that in the event of war with an "informatized" country (e.g., the United States), the enemy's political system, economic potential, and strategic objectives

92 Bryan Krekel et al., *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, p. 14. Emphasis added.

will be primary targets for cyber attack.[93] This thinking is not new. As far back as 2000, Chinese military analyst Wang Huacheng described U.S. reliance on information technology and space as its "soft ribs" and a source of "strategic weakness."[94]

China's doctrinal, material, and operational emphasis on cyber war strongly suggests that in a conflict with the United States or any other power (e.g., Japan or Taiwan) China is preparing to exploit the dependence of the advanced economic powers on computer systems and networks. China's persistent cyber reconnaissance activities, which likely include efforts to pre-position logic bombs[95] in key locations in the U.S. critical infrastructure, are examples of

93 Thomas, "Google Confronts China's 'Three Warfares,'", p. 109.

94 "U.S.-China Economic and Security Review Commission," *2008 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2008), p. 156.

95 A logic bomb (also referred to as "slag code") is code that is added to the software of an application or operating system that lies dormant for a predetermined period of time where upon it becomes active, or "explodes." Viruses programmed to be released at a certain time are logic bombs. They can reformat a computer's hard drive, and delete, alter, or corrupt data. An attempted logic bomb attack occurred at mortgage finance company Fannie Mae in 2008. The attack, which was foiled, would have decimated all the company's roughly 4,000 servers, causing millions of dollars in damage and shutting down Fannie Mae for a least a week. The logic bomb was planted by an employee on the day he was fired from his job but who was permitted to finish out the day, thus giving him access to the computer network. Fortunately, the logic bomb was discovered and "defused." Had it not been, the bomb would have erased all the data on all of Fannie Mae servers, overwriting the data with zeroes. Kevin Poulsen, "Fannie Mae Logic Bomb Would Have Caused Weeklong Shutdown," *Wired*, January 29, 2009, available at http://www.wired.com/threatlevel/2009/01/fannie/, accessed on March 3, 2012; Klimburg, "Mobilising Cyber Power," p. 42; and Bruce Schneier, "Thwarting an Internal Hacker," *Wall Street Journal*, February 16, 2009, available at http://online.wsj.com/article/SB123447990459779609.html, accessed on March 30, 2012.

its emphasis on deception, and also reflect Sun Tzu's admonition to "win victory before the first battle."[96]

Arguably, the case can be made that non-kinetic cyber attacks aimed at paralyzing an enemy country's economy and triggering social turmoil would not represent "fighting" in the sense of being large-scale engagements between traditional forces.[97] Viewed in this manner, cyber warfare can be a means of achieving victory without fighting.

Toward this end the Chinese have adopted a formal cyber war strategy called "Integrated Network Electronic Warfare" (INEW).

> INEW consolidates the offensive mission for both computer network attack (CNA) and [electronic warfare] under PLA General Staff Department's (GSD) 4th Department (Electronic Countermeasures), while the computer network defense (CND) and intelligence gathering responsibilities likely belong to

96 As Vice Admiral (Retired) Michael McConnell observed: "Since the late 1990s, China has systematically done all the things a nation would do if it contemplated having an offensive cyber war capability and also thought it might itself be targeted by cyber war; it has . . . laced U.S. infrastructure with logic bombs." Clarke et al., *Cyber War*, p. 54. See also Andress et al., *Cyber Warfare*, p. 44; Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, April 8, 2009, available at http://online.wsj.com/article/SB123914805204099085.html, accessed on March 30, 2012; and Andy Greenberg, "Spies in the Grid: The Feds' Timely Cyber Alarm," *Forbes.com*, April 8, 2009, available at http://www.forbes.com/2009/04/08/hackers-utilities-cybersecurity-technology-security-power-grid_print.html, accessed on April 17, 2012.

97 Thomas, "Google Confronts China's 'Three Warfares,'" p. 110.

the GSD 3rd Department (Signals Intelligence), and possibly a variety of the PLA's specialized information warfare (IW) militia units."[98]

The INEW strategy emphasizes precision targeting and disciplined coordination to strike carefully selected nodes of an enemy's information systems to achieve maximum impact.[99] The goal is to establish control over the adversary's ability to access or disseminate information. This seems to place a premium on the Chinese intelligence service's ability to accurately map its adversaries' military and critical infrastructure networks prior to a conflict. To the extent this can be accomplished, it could reduce the number of logic bombs required to achieve the desired effects, while also enhancing the prospects of creating catastrophic levels of destruction against a target state.

Cyber operations involving CNA combined with EW are apparently perceived to be "bloodless" by at

98 Krekel et al., *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, pp. 6-7. Additionally, some 250 hacker groups have been identified operating within China, comprising perhaps thousands of individual hackers. The People's Liberation Army sponsors hacking contests as a way of identifying promising cyber warriors—and to keep this talent occupied in ways that do not threaten the regime. See Klimburg, "Mobilising Cyber Power," pp. 46-47.

99 Klimburg "Mobilising Cyber Power", p. 40.

least some PLA cyber warfare strategists, and thus not likely to trigger a forceful response.[100] An example of this way of thinking can be found in the writings of Chinese military theorists Colonel Long Fangcheng and Senior Colonel Li Decai, who appear to embrace the dangerous assumption that a cyber attack on another nation's economy will not lead to any large-scale response.[101]

In addition to cyber attacks against enemy critical infrastructure targets at the "strategic" level of war, as in the case of Russia, it appears Chinese leaders believe that cyber attacks can have a significant effect at the operational level of warfare. For example, the PLA discusses employing cyber attacks to fracture the integrity of enemy C4ISR systems and battle networks.[102] This is significant, as the majority of U.S. military logistics information systems are transmitted or accessed via unsecure networks.[103]

100 Ibid., p. 19.

101 Thomas, "Google Confronts China's 'Three Warfares,'" p. 110.

102 Timothy L. Thomas, "China's Electronic Long-Range Reconnaissance, *Military Review*, November-December 2008, p. 48.

103 Krekel et al., *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, p. 24.

Chinese Cyber Operations

Titan Rain

For at least the past decade, the Chinese have engaged in aggressive and intrusive cyber reconnaissance activities. Beginning in 2002, Chinese cyber forces engaged in a campaign that saw them penetrate Sandia National Laboratories, the U.S. Army Information Systems Engineering Command, and other sites in an operation known as Titan Rain.[104] Titan Rain is the name of a Chinese scanner program that probes national defense and high-tech industrial computer networks looking for vulnerabilities.[105]

The operation was highly sophisticated. Chinese military hackers managed to penetrate systems without committing any keystroke errors or leaving digital fingerprints. They were also able to create a clean backdoor exit, all in under 20 minutes. These skills are comparable to the best demonstrated by militaries or intelligence agencies with advanced cyber skills.[106]

104 Menn, *Fatal System Error,* p. 217. Titan Rain also involved attacks on sites in the United Kingdom.

105 Posner, "China's Secret Cyberterrorism," p. 2

106 Ibid.

Titan Rain's objective was to exfiltrate sensitive data. Once the targeted computer system was penetrated, everything on its hard drives was copied and sent to computers in South Korea, Hong Kong, and Taiwan. From there it was routed to computers in China's Guangdong province.[107] Remarkably, the Titan Rain campaign was not uncovered by U.S. cyber security until 2007.[108] Thus, for at least five years the Chinese had been able to engage in what appears to have been a highly successful espionage effort that could also be viewed as an act of economic warfare.

Aurora

The Aurora cyber attack campaign was likely waged between the middle and end of 2009. In early January 2010 Google announced that a computer attack originating in China had penetrated its corporate infrastructure (in mid-December 2009) and stolen information from its computers, most likely source code.[109] As with Titan Rain, the campaign demonstrated a

107 Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," p. 55.

108 Paul Cornish, David Livingstone, Dave Clemente, and Clair Yorke, *On Cyber Warfare* (London: Chatham House, 2010), p. 8.

109 Thomas, "Google Confronts China's 'Three Warfares," p. 101; and Michael Joseph Gross, "Enter the Cyber-Dragon," *Vanity Fair*, September 2011, p. 49.

high level of sophistication characteristic of an advanced persistent threat (APT)[110] attack.

Generally similar to Titan Rain, the cyber campaign involved operations designed to penetrate secure computer systems, whereupon the attackers exfiltrated data. Among the victims was Google. The attackers exfiltrated the source code for a Google password-management program called Gaia.[111]

In June 2011 Google announced that hundreds of its users had been victims of a "spear phishing" operation.[112] Such an operation begins with the attacker undertaking cyber reconnaissance to identify information about a company's employees, targeting or "spearing" them individually. Google traced the attacks to Jinan, a Chinese city that serves as a base for the PLA, and the location to which previous cyber attacks had been traced. In this case the

110 The term "advanced persistent threat" is typically associated with capabilities demonstrated at a scale and level of sophistication requiring the resources of a nation-state.

111 In gathering source code, sometimes referred to as the "secret sauce" or "virtual DNA" of an IT firm like Google, it becomes easier for cyber warriors to discover new vulnerabilities in a Web application that can facilitate future attacks. Recall that China also has Microsoft's source code. Chinese nationals employed by Google may have aided the Chinese attack. After the attacks were discovered, Google denied some of its China employees access to internal networks. Others were put on leave or reassigned. Gross, "Enter the Cyber-Dragon," pp. 49-50.

112 L. Gordon Crovitz, "China Goes Phishing: Google uncovers Beijing's escalating cyber warfare," *Wall Street Journal*, June 6, 2011, p. A17. For a discussion of how the attackers penetrated cyber defenses and a discussion of possible cyber security enhancements, see McAfee Labs and McAfee Foundation Professional Services, *Protecting Your Critical Assets: Lessons Learned from 'Operation Aurora'* (Santa Clara, CA: McAfee, Inc., 2010).

Chinese likely trolled social-networking sites, such as Facebook and LinkedIn, or researched email archives exfiltrated in previous attacks. Using this information the Chinese were able to develop profiles of their targeted individuals. The Chinese next crafted emails or other messages specifically tailored to the targets. These were then sent to the target using false identities of individuals whom the target trusted.

The messages contained malicious attachments, in some cases armed with a zero-day exploit.[113] If the targeted individual clicked on the attachment, the malware, a remote-access tool, or "rat," attached itself to the user's Windows operating system. In the case of Aurora, the cyber payload established a backdoor connected to command and control servers in Taiwan.[114] In this way the Chinese penetrated the targeted individual's company's firewalls. The attacker

113 A zero-day exploit is defined as a cyber security vulnerability that is exploited or used on the same day that the vulnerability becomes generally known. As the term implies, there are zero days between the time the vulnerability is discovered and when the cyber attack exploiting the vulnerability occurs. A zero-day exploit can also be defined as an cyber attack that exploits a vulnerability (e.g., in Microsoft's Windows operating system) before that vulnerability is known. Thus zero days in this case refers to the fact that there are zero days between the exploit of the cyber vulnerability and an awareness of the vulnerability by either the software writer or the target of the cyber attack.

114 McAfee Labs, *Protecting Your Critical Assets: Lessons Learned from 'Operation Aurora'*, p. 3.

manually operated the rat to gain access to other parts of the computer network and exfiltrate data.[115]

Google reported that Aurora's spear phishing targets were "senior U.S. government officials, Chinese political activists, officials in several Asian countries (predominantly S. Korea), military personnel and journalists."[116] After cyber security experts identified similarities between the tools used in Aurora attacks and malware tools that were posted on open Chinese hacker forums, suspicion increased that the Chinese government was using "volunteers" as proxies to launch the attacks, somewhat analogous to the Chinese "volunteer" military units that attacked U.N. forces in the Korean War.[117] Attention centered on the Lanxiang Vocational School, which has close ties to the PLA, to include providing it with cyber recruits.[118]

Google was not the only target of the cyber assault. There were reports that similar spear phishing attacks had been conducted against Microsoft's Hotmail and Yahoo's email services.[119] The campaign

115 Gross, "Enter the Cyber-Dragon," p. 51.

116 Crovitz, "China Goes Phishing: Google uncovers Beijing's escalating cyber warfare."

117 Gross, "Enter the Cyber-Dragon," p. 51.

118 Thomas, "Google Confronts China's 'Three Warfares,'" p. 105.

119 Crovitz, "China Goes Phishing: Google uncovers Beijing's escalating cyber warfare."

also apparently involved attacks on dozens of other organizations, to include Adobe Systems, Juniper Networks, Rackspace, Dow Chemical, Morgan Stanley, Northrop Grumman, and Symantec.[120]

To use traditional military terminology, the Aurora campaign can be viewed as a kind of reconnaissance or espionage operation in which Chinese cyber experts were employed to gather information about competitors, somewhat similar to the activities of a spy or satellite. If the information acquired could be employed to enhance China's economic competitiveness (e.g., proprietary information regarding a firm's bid on a project for which the Chinese were competing, proprietary industrial processes, etc.) it might also be viewed as a form of economic warfare. Most important for our purposes, as the skills and techniques associated with cyber espionage and economic warfare are very similar to those needed to emplace logic bombs, the potential effects could ultimately be far greater.

120 Thomas, "Google Confronts China's 'Three Warfares,'" p. 103.

Night Dragon

Beginning in November 2009 a series of coordinated, covert cyber attacks, known as Night Dragon, were launched against global oil, energy, and petrochemical companies. The attackers leveraged spear-phishing and Microsoft Windows operating system vulnerabilities to exfiltrate intellectual property. Once again, the attacks are believed to have originated in China.[121]

Shady Rat

About the same time as operations Aurora and Night Dragon were identified, security experts uncovered an operation in which the attacker seemed to be "motivated by a massive hunger for secrets and intellectual property; this is different from the immediate financial gratification that drives much of cybercrime..."[122] The operation, named Shady RAT,[123] targeted over seventy victims in fourteen different countries. As in the case of Night Dragon, the penetrations were accomplished through spear-phishing

121 "Global Energy Cyberattacks: 'Night Dragon,'" *McAfee White Paper*, February 10, 2011, p. 3.

122 Alperovitch, "'Revealed': Operation Shady RAT," p. 2.

123 The term "RAT" stands for "remote access tool."

in which an email containing an exploit was sent to an individual with access to a network. When the email was opened, malware was downloaded that set up a backdoor communications channel to a command and control server. Then it began the exfiltration of information from the infected machine or network. The information compromised included national secrets, source code, databases and SCADA configurations. According to one security firm, the result of this operation has been "nothing short of a historically unprecedented transfer of wealth."[124] According to one cyber security expert, "All the signs point to China" as the source of the penetrations.[125]

NORTH KOREA

It took North Korea decades to develop its nuclear capability, an exceedingly modest one at that. Such is not the case with its cyber arsenal, which while apparently modest seems to have been developed over a far shorter period of time and at far less cost.

124 Alperovitch, "'Revealed': Operation Shady RAT," p. 2.

125 Michael Joseph Gross, "Exclusive: Operation Shady RAT—Unprecedented Cyber-espionage Campaign and Intellectual-Property Bonanza," *Vanity Fair*, August 2, 2011, available at http://www.vanityfair.com/culture/features/2011/09/operation-shady-rat-201109, accessed on January 28, 2012. See also Gross, "Enter the Cyber-dragon."

The first serious indicators of Pyongyang's status as a cyber power occurred in 2009 when the South Korean banking system was subjected to DDoS attacks originating in North Korea. Similar attacks occurred in 2011; however, the new strikes were nearly an order of magnitude greater in their intensity. Under the weight of the DDoS attacks, nearly half of the servers of one South Korean bank crashed in less than one day in April.[126] This left some 30 million customers of the Nonghyup agricultural bank unable to use automated teller machines (ATMs) or online services for several days. Perhaps more worrisome is that some of the bank's key data were also either corrupted or destroyed.[127] One cyber expert who analyzed the attack concluded the North Koreans "are doing massive damage with simple means. This is Cyberwarfare 101."[128]

Forensics undertaken by cyber security personnel found that the attack was made possible by a contractor who inadvertently downloaded malware onto a laptop computer with access to the bank's

126 Chico Harlan and Ellen Nakashima, "Suspected N. Korean Net Attack Raises Fears," *Washington Post*, August 30, 2011, p. 1.

127 Ibid.

128 Ibid.

computer system.[129] This gave the hackers access to the system. Over time the North Koreans inserted malicious code into the bank's computer network, enabling them to launch a simultaneous attack on hundreds of servers and crash the system.

Some South Korean officials fear that North Korea is seeking to develop the capability to inflict far greater damage on the computer networks that oversee the nation's critical infrastructure. As evidence they cite the arrest in 2010 of an alleged North Korean spy accused of seeking confidential information regarding Seoul's railway system, which uses the same kind of industrial software controllers targeted by Stuxnet.[130]

What does this suggest? Perhaps not much. Some mix of Russian organized crime organizations, patriotic hackers, and quite possibly the Russian government demonstrated in Estonia how DDoS attacks could disrupt a nation's banking system, at least temporarily. And as noted earlier in this study, there have been earlier attacks on power grids and other critical infrastructure elements. What may prove significant

129 Ibid., p. 2.

130 Ibid.

is North Korea's ability to execute a fairly sophisticated cyber attack despite its status as one of the world's most backward nations, especially when it comes to its IT infrastructure and the IT literacy of the vast majority of its people. It could be that Pyongyang "rented" the botnets that produced the DDoS attacks, and perhaps the malware involved in the more recent attack. If so, it again demonstrates the impressive cyber capabilities of certain non-state actors. On the other hand, if the effort was entirely indigenous to North Korea, it suggests the barriers to becoming a modest cyber power are relatively low.

Summary

With the rise of cyber crime as a full-fledged "industry" some governments, especially that of Russia, appear to have joined with cyber criminals in an alliance of sorts. Absent such relationships it becomes difficult to explain how, despite their involvement in cyber crime, cyber criminals like those running RBN have escaped prosecution. They are free because Moscow sees them as a kind of latter-day privateers, modern-day Sir Francis Drakes raiding the

developed countries of the Western world, not for gold and silver, but for other forms of financial gain, to include intellectual property. Organizations like RBN are thus free to reap financial gains in their attacks against Western societies, while recruiting and training cyber criminals who can also serve, when need be, as cyber warriors for the state.

They may also be engaged, directly or indirectly, in Russian efforts to steal intellectual property, state secrets, and other sensitive information (e.g., data regarding bids on major business initiatives against which Russian government entities, like Gazprom, plan to bid).[131] There is doubtless some satisfaction derived from the Russian ruling class, a significant number of whom served in the country's secret police and intelligence services during the Cold War, that after the long humiliating years following the collapse of the Soviet Union they can wage a generally successful economic war against their once (and perhaps current) enemies.

China is almost certainly engaged in cyber economic warfare and espionage against the West in

131 Carr et al., *Project Grey Goose*, p. 12.

general, and the United States in particular. Rather than leveraging organized crime, however, Beijing appears to favor a kind of cyber militia or cyber volunteers. In 2003, for example, China's Hauwei Shenzhen Technology Company, whose CEO is a former PLA member, was charged with stealing secrets and wholesale pirating of Cisco software, a U.S. firm.[132] Four years later Huawei unsuccessfully attempted to buy 3Com, a U.S. company which supplies the U.S. government with security software, routers, and servers. India turned down a $60 million Huawei investment deal in 2005 after concerns over cyber reconnaissance, noting that Huawei is the same company that conducts sweeping and debugging of the Chinese embassy.[133] At the time, India's Defence Ministry stated, "the choice was between cheap Chinese equipment and national security."[134] A year later the U.S. State Department announced that its Lenovo computers would not be authorized to store classified data or be linked

132 Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," p. 68.

133 Ibid.

134 Ibid.

to classified networks owing to cyber security concerns.[135] Recently the Australian government has refused to allow Huawei to bid on work for its National Broadband Network.[136]

Western democracies have responded to the rise of cyber crime, and to the growth of cyber economic warfare. In February 2005, a group of chief information officers from both hardware and software companies—among them Microsoft, Dell, IBM, Hewlett-Packard, and security giant Symantec—met with senior U.S. Government officials to secure support against the rising tide of cyber attacks on them and on Americans in general.[137] Yet two years later the Center for Strategic and International Studies reported that cybercrime had risen to the level where

135 Lenovo, a Chinese firm, acquired IBM's Personal Computing Division in 2005. A year later Lenovo began lobbying activities directed at the U.S. Congress, some of whose members had raised concerns over its efforts to penetrate the U.S. Government's personal computer market. From 2006-2009, Lenovo spent over $1 million for U.S. firms to engage in lobbying Congress on its behalf. Lenovo also spent over $2.5 million over the same time period on its own direct lobbying efforts. See "The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector," U.S-China Economic and Security Review Commission, January 2011, pp. 66-68; and Greg Keizer, "Lenovo Denies Its PCs Are Security Risk," *CRN*, May 26, 2006, available at http://www.crn.com/news/security/188500323/lenovo-denies-its-pcs-are-security-risk.htm?pgno=1, accessed on March 5, 2012.

136 Geoffrey Barker and David Ramli, "China's Huawei Banned From NDN," *Australian Financial Review*, March 24, 2012, available at http://www.afr.com/p/technology/china_giant_banned_from_nbn_9U9zi1oc3FXBF3BZdRD9mJ, accessed on April 14, 2012; and Oonagh Reidy, "Huawei Begs NBN Mercy On Cyber War Fears," *Smarthouse*, March 27, 2012, available at http://smarthouse.com.au/Wireless_And_Networking/Industry/M9C4K6E6, accessed on April 14, 2012.

137 Menn, *Fatal System Error*, p. 222.

it constituted a threat to national security.[138] The report's authors declared

> we are in a long-term struggle with criminals, foreign intelligence agencies, militaries and others . . . [T]his struggle does more real damage every day to the economic health and national security of the United States than any other threat...[putting cyber security] on par with weapons of mass destruction and global jihad.[139]

138 Ibid.

139 CSIS Commission on Cybersecurity for the 44th Presidency, "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies, 2008, pp. 15, 77.

CHAPTER 4 > CYBER WAR AND CATASTROPHIC DESTRUCTION

The preceding chapter outlined some of what is known from open-source materials regarding cyber weapons' growing abilities to inflict damage on individuals, businesses, societies, and their governments. We now tighten the focus to explore the potential of cyber weapons to inflict prompt, catastrophic destruction.

The chapter opens with a general discussion of computer network vulnerabilities, followed by a brief examination of the prospective vulnerabilities of two key elements of the critical infrastructure: the power grid and the financial system. The discussion then turns to two examples of the growing sophistication of cyber weaponry.

COMPUTER NETWORK VULNERABILITY

To execute a successful attack in the cyber domain, the attacker must defeat or circumvent the defenses arrayed against him. In the case of cyber defenses, there exist several major areas of weakness. The first is the relative prevalence of single points of failure, such as a SCADA system that regulates some key process or function. In many complex systems, compromising these single points of failure can bring an entire process or facility to a swift halt.

Cyber attacks can be launched to degrade the performance of such systems and networks. If the attacks succeed, they can cause portions of the system or the network to function poorly, in an erratic manner, or not at all. At a minimum, the defender can spend an inordinate amount of time troubleshooting and rectifying the problem. It may be possible to cause SCADA systems to deviate from their baseline, leading to the malfunction of the production system they are regulating, gas pipelines, or power generators.[140]

Protecting single-point failure systems and networks requires a defense in depth since, by definition,

140 Clarke et al., *Cyber War*, p. 70.

their function cannot be sustained without them. The question then becomes whether such a defense can either defeat an attack or require the attacker to commit more resources to the attack than he hopes to gain from its success. In the second case, a "rational" attacker would be deterred from attacking. However, the cyber competition appears to be an offense-dominant competition.[141] That is to say that if both the attacker and defender are given equal resources, the attacker will prevail. Those seeking to defend single points of failure from cyber attack find themselves confronting the unenviable situation of investing more resources than the attacker in the futile hope that they can defeat all attacks (as any one successful attack will compromise their system).

Unable to mount a perfect defense, or a defense that cannot be compromised more cheaply by a determined attacker, many businesses—including those associated with critical infrastructure—engage in

141 It is unlikely that cyber criminals would persist in their activities if the competition favored the defense. In that case, crime would "not pay." The situation is less clear in the case of targets such as SCADA systems, where there is no clear payoff compared with DDoS attacks to extort funds from an online business (e.g., gambling site) or identity theft. (That said, it is conceivable, for example, that successful attacks on SCADA systems regulating a portion of the power grid could enable the attacker to extort payments in return for discontinuing such attacks.) In the case of monocultures (e.g., Microsoft's Windows Operating System) the environment is "target rich" in the sense that the OS has tens of thousands of zero-day vulnerabilities. To gain access to a computer the attacker merely has to identify one such vulnerability whereas the defender must identify and patch all of them.

risk management. This involves trying to implement defenses that are sufficiently robust relative to those protecting other similar targets in the hope that an attacker will strike a relatively more vulnerable target. Alternatively, a defender might seek to invest just enough in the way of defenses so as not to exceed the cost of recovering from a successful attack (or series of successful attacks).

A second major kind of weakness is a network's reliance on a software monoculture that, once penetrated, can trigger a cascade failure. This kind of failure is relatively easy to detonate in a monoculture, an example of which is the Microsoft Windows operating system that is prevalent on most computers, as the firm enjoys over an 85 percent average market share.[142] Microsoft's principal application, Microsoft Office, commands over 90 percent of the market.[143] Similarly, Intel boasts a market share in excess of 80 percent for its chips (with AMD having over 15

142 See "Top Operating Systems Share Trend," NetMarketshare, available at http://www.netmarketshare.com/os-market-share.aspx?qprid=9, accessed on March 1, 2012. Note, however, that there are different versions of Windows being used. This may complicate the attacker's problem significantly.

143 Jason Mick, "Office 2010 to Launch Today, Microsoft Owns 94 Percent of the Market," *Daily Tech*, available at http://www.dailytech.com/Office+2010+to+Launch+Today+Microsoft+Owns+94+Percent+of+the+Market/article18360.htm, accessed on March 1, 2012.

percent of the roughly remaining 20 percent).[144] Creating a culture in which most systems and key applications are almost entirely alike promotes efficiency and reduces cost, hence their attraction. However, given this kind of monoculture, the attacker only needs to find one way of penetrating his target (e.g., Microsoft's Windows 7 operating system). Once that has been accomplished, all systems running on that operating system can have their defenses penetrated, assuming the penetrations occur sufficiently close in time as to preclude the development and dissemination of a patch—and that the patch is applied promptly. As with the challenge associated with single points of failure, the defender is faced with the need to engage in risk management between the efficiency gains and cost reductions associated with running its computer systems on the Windows operating system and the costs that might be incurred if the system is penetrated by a cyber attack. As in the case of single point of failure, the

144 Paul Lilly, "Intel's Market Share Further Ahead of Pack after Crossing Sandy Bridge," *Hot Hardware*, September 28, 2011, available at http://hothardware.com/News/Intels-Market-Share-Further-Ahead-of-the-Pack-after-Crossing-Sandy-Bridge/, accessed on March 1, 2012; and Agam Shah, "Intel Loses Laptop Chip Market Share to AMD in Q3," *PC World*, November 3, 2011, available at http://www.pcworld.com/article/243114/intel_loses_laptop_chip_market_share_to_amd_in_q3.html, accessed on March 1, 2012.

defender here would also balance the cost of fielding cyber defenses against the cost of recovering from the range of prospective cyber attacks, from those causing minor inconvenience to those that effectively destroy the system, along with the probabilities of their occurrence.

As discussed in the preceding chapter, a successful cyber attack that enables the attacker to access a computer or computer network can result in a range of negative consequences. For example, the attacker may manipulate the data stored in the system to cause subtle degradation, such as changing the results of medical tests, altering financial data, and targeting transportation location systems, all of which could be difficult to detect while resulting in substantial damage.[145] Of course, the attacker could also exfiltrate or destroy data, or commandeer the computer or network for employment as part of a botnet.

A third major vulnerability in cyber defense stems from the use of global supply chains for the components that comprise computers, their networks, and the control systems they monitor. For example,

145 Andress et al., *Cyber Warfare*, p. 176.

absent the production of computer hardware and software in controlled environments, it may be difficult if not impossible to ensure that they have not been modified to enable cyber penetration of the systems in which they will be employed.[146] China is manufacturing microchips for dozens of major international companies, and those chips could hold viruses set to activate when used in a computer network.[147] China's microchip output is almost doubling every two years. Chip giant Intel, for instance, has opened a multibillion-dollar plant in Dalian, China.[148]

Finally there is the problem of defending against a cyber attack mounted by an insider; that is, a person who has been given access to the computer system or network targeted for attack. In earlier times such individuals were called traitors or

146 Melissa Hathaway, *Strategic Advantage: Why America Should Care About Cybersecurity* (Cambridge, MA: Harvard Kennedy School, 2009), p. 7.

147 Posner, "China's Secret Cyberterrorism," p. 2.

148 Ibid. See also Markoff, "Old Trick Threatens the Newest Weapons." Only one-fifth of all computer chips are made in the United States. The Defense Department buys only about 2 percent of its computer chips from secure facilities based in the United States. While the Pentagon is expanding the number of plants authorized to manufacture chips for it under the Trusted Foundry Program, production cannot meet the demand for chips for classified military systems. Today's computer chips have billions of transistors, enabling subtle modifications in manufacturing or in the design of chips virtually impossible to detect. Tampered chips could contain hidden "kill switches" that could disable the chip's ability to perform its function when needed. There are reports that the Israeli air attack on Syria's nuclear reactor in September 2007 was enabled by embedded kill switches in the Syrian air defense network that caused it to malfunction.

fifth-columnists.[149] Perhaps even more important, there also is the problem of defending against the unwitting person who fails to follow appropriate security practices and who unintentionally inserts a Universal Serial Bus (USB) thumb drive containing a virus into a network. These individuals are prime targets for spear phishing, and could inadvertently insert malware directly into the systems to which they have access, thereby modifying, extracting, or destroying data. To be effective, those charged with establishing cyber defenses must stop all attacks in each of the four areas of weakness described here, while the attacker must succeed only once.

Aside from gaining entry, there are other ways to prevent a computer system or network from functioning effectively, such as DDoS attacks undertaken by botnets. Some experts have concluded that as computing power continues to grow along the lines described in Moore's Law,[150] it will soon be possible (if

149 A fifth column refers to members of a state who attempt to assist a foreign power in undermining their government from within. The term "fifth column" is a reference the military use of a column of soldiers four across when marching. The fifth column is the unseen column at work from within the enemy's own ranks.

150 Moore's Law originated with Intel Corporation's Gordon Moore in a paper written in 1965. In it Moore observed that the number of components in integrated circuits had doubled every year from the invention of the integrated circuit in 1958 through 1965. Moore predicted this trend would hold for at least another decade. As a rule of thumb, the "law" has proven remarkably accurate.

it is not possible already) for even non-state entities to assemble botnets with massive computing power. (As we shall, the Conficker virus, which is believed to have been developed by a non-state entity, assembled millions upon millions of computers in its botnet.)[151] Were such a botnet put to work as part of a single concerted effort, its computing power could crack many codes, breaching online database defenses to extract, distort, or corrupt data. An attacker could potentially go even further and "destroy" the computer system or network by deleting its data.[152] This kind of computing power could penetrate key parts of a country's vital modern infrastructure: computer systems that control telephones, energy flow, air traffic, healthcare information, financial data—even the Internet itself.[153]

151 Mark Bowden, "The Enemy Within," *The Atlantic*, June 2010, available at http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/, accessed on January 10, 2012.

152 Note that when a zombie computer functioning as part of a botnet is put to work breaking a code, more computing power is employed. This increases the risk that the zombie's activity becomes obvious to the user, who at some point can be expected to take remedial action, if only to turn the computer off in frustration. On the other hand, if the code breaking consumes only a little computer power, it will take much longer to accomplish its mission. I am indebted to Herbert Lin for this observation.

153 John Morrison, *White Paper: The Why and How of Cyber Ranges* (Bethesda, MD: Lockheed Martin, 2010,) p. 2. Cyber attacks are also capable of producing physical destruction. For example, a water-driven electrical generator at Russia's Sayano-Shushenskaya dam, near the city of Cheremushki, was physically destroyed due to a cyber event in August 2009. It occurred when one of the dam's 10,650-megawatt 1,000-ton hydroturbine generators was remotely restarted by a computer operator while the generator was being serviced. The generator began spinning, rising some 50 feet into the air before exploding. Over 70 people were killed in the accident, which also destroyed eight of the remaining nine generators at the dam. Bill Gertz, "Computer-Based Attacks Emerge As Threat of Future, General Says," *Washington Times*, September 13, 2011, available at http://www.washingtontimes.com/news/2011/sep/13/computer-based-attacks-emerge-as-threat-of-future-/?page=all#pagebreak, accessed on March 3, 2012.

CYBER ATTACKS

In the case of a sophisticated cyber attack, the attacker will likely not use exploits that are available to the general public (e.g., those that are posted on the Internet), as such methods are likely to have already been patched or mitigated in some fashion, and easily deflected by well-defended systems. Rather, the attacker will likely employ zero-day exploits which stand a much greater chance of success due to their not being commonly available (although advertisements for "zero days" can be easily found on the Internet). Once a system has been penetrated, the attacker can plant hidden logic bombs.

Depending on the nature of the attack and the attacker's characteristics, it may be important to test these exploits in an environment as close as possible to the actual target. This may be especially important where the attacker is trying to create catastrophic effects. In such instances, the attacker (assuming it is the government of a state) may risk large-scale retaliation from the defender in the wake of the attack. The risks may be worth it to the attacker if the prospective benefits of the attack are likely to be

realized. Mapping the computer network infrastructure of a nation's critical infrastructure sufficiently to enable a cyber attack that triggers catastrophic consequences seems likely to require the services of a highly capable intelligence apparatus, the kind only major nation-states can afford to assemble and maintain. The ability to test the exploit (or exploits) can enable the attacker to determine whether the exploits will achieve the desired effect (including prospective second-order effects), and aid in developing contingency plans to compensate for problems that might be encountered.

Second-order effects may be a source of particular concern, as the precise configuration of an adversary's computer network may be difficult to discern through the Internet. For example, it can be difficult to disrupt a particular computer without affecting other computers that are connected to it. A case in point may have occurred in 2008, when the U.S. military allegedly conducted a cyber attack to dismantle a Saudi Web site that U.S. officials believed was supporting suicide bomber operations in Iraq.[154]

154 Ellen Nakashima, "U.S. Eyes Preemptive Cyber-Defense Strategy," *Washington Post*, August 29, 2010, p. A5.

The attack inadvertently disrupted more than 300 servers in Saudi Arabia, Germany, and Texas. This pales in comparison to the breadth of cyber attacks that would occur in an operation designed to inflict catastrophic destruction on a major economic power. It also points out the importance of testing in preparation for a general conflict involving more than cyber weapons. Here high-fidelity cyber weapons testing may enable planners to determine the best mix of weapons (and the required level of attack redundancy), be they kinetic or non-kinetic. Toward this end, high-fidelity cyber training ranges could be a key source of competitive advantage, as could lessons learned from "precursor" cyber campaigns such as those waged against Estonia and Georgia (again, assuming Russia was the originator).[155]

Non-state groups, however, especially those whose objective is simply to terrorize and to cause destruction, are likely to be far less interested in testing their weapons. Such groups will likely have little in the way of assets against which to retaliate, nor care if their attack triggers harmful second-order effects.

155 In cases where SCADA systems are targeted, they would need to be obtained for cyber range-test exercises.

They may, however, be restrained somewhat if they are being employed as a proxy by a state sponsor. To the extent that the state sponsor is concerned about possible undesirable or unintended second-order effects of a cyber attack, it could attempt to prevent its proxy from executing such attacks.

Looking further into the future, there exists the possibility that states and non-state entities will develop autonomous cyber attack weapons. These weapons would, in theory, be an offshoot of malware, and would exist with the express purpose of attacking a particular target or targets. Their originators would likely take steps to ensure they can control such tools to prevent attacks against targets other than those specifically designated by their masters. It seems likely that developing effective control measures would require tests of the control system, as well as of the effects the weapons would have against their targets.

Yet it is not clear that such control systems would be fail proof. For example, today's botnets do not demonstrate independent aggressive behavior, instead waiting for the command of the botnet operators.

There are, however, no inherent barriers to botnets being configured to operate autonomously without human guidance.[156] A cyber competitor operating such systems could potentially find cyber weapons being employed unintentionally. These weapons could even be turned on their owner if the control mechanism is compromised. This may be a primary reason why such weapons are not set to be capable of autonomous operation. Should unauthorized attacks start it may prove difficult or even impossible to terminate them. In this regard creating autonomous cyber strike forces recalls the "Dead Hand" nuclear retaliatory system considered by Soviet leaders in the early 1980s.[157]

DEFENSE AGAINST CYBER ATTACK

As the cyber competition appears to favor the offense, and potentially by a considerable margin, even a cyber defense with access to an unlimited budget

156 Andress et al., *Cyber Warfare*, p. 204.

157 The "Dead Hand" was an option explored by the Soviet Union's leadership in the latter stages of the Cold War. It called for a system in which a computer would be empowered to launch a retaliatory strike against the United States in the event the leadership was unable to do so (e.g., as a consequence of a U.S. "decapitation" attack that either killed the leadership, destroyed the leadership's ability to communicate with Soviet nuclear forces, or both). David E. Hoffman, *The Dead Hand* (New York: Anchor Books, 2009), p. 23. The concept was never implemented.

could not eliminate the possibility of intrusions, as new vulnerabilities are constantly being identified. General Alexander summed up the competition well when he stated "In cyberspace the only 'perfect' defense is the static one: to disconnect [from networks] and thereby forfeit the cyber realm and its economic and social benefits to one's adversaries."[158]

Mounting a serious defense against a major cyber attack would likely require, at a minimum, intrusion detection and intrusion prevention on a nationwide scale. This seems unfeasible, however, as the networks that comprise the Internet are typically not segmented along national boundaries. Put another way, there are no national borders when it comes to the cyber world. Even if there were and the United States could close its virtual cyber borders to traffic coming in from the outside, the attack could be generated from within its borders (i.e., originate within the United States using the Internet or insider access), and there is as of yet no effective means to prevent such an attack from occurring.[159]

158 Keith B. Alexander, testimony before the House Armed Services Committee, September 23, 2010, p. 7.

159 Andress et al., *Cyber Warfare*, p. 200.

That said, there are two primary options for fielding more effective defenses to provide intrusion detection or defense on a national scale. One option is to structure networks to provide a limited number of connections from the external environment to the area to be defended and monitored. This would require restructuring existing networks on a massive scale, and would likely be prohibitively expensive. It seems unlikely that this kind of effort would be undertaken absent some major catalytic event, such as a cyber attack that produced catastrophic damage. The second option would be to move to massively distributed Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS).[160] This would have the advantage of using existing networks, but would be both costly and likely fail to intercept at least some of the hostile cyber activity entering and exiting these networks.[161] As neither of these options would provide an airtight barrier to cyber attacks

160 "An *intrusion detection system* (IDS) is software that automates the intrusion detection process. An *intrusion prevention system* (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents." Karen Scarfone and Peter Mell, Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)* (Gaithersburg, MD: Department of Commerce, Computer Security Resource Center, National Institute of Standards and Technology, February 2007), p. ES-1.

161 Andress et al., Cyber Warfare, pp. 187-188.

through the Internet, security at the end nodes would remain an important component of cyber defense.

It is far from clear that, at least in the United States' case, the defenses that are available are being used effectively, either in terms of identifying that a computer system is under attack or providing internal security. Verizon's 2009 Data Breach Investigations Report included two particularly instructive findings. First, the report showed that 75 percent of all data losses from cyber attacks are not discovered by a firm's cyber security staff, but by unrelated third parties.[162] Second, it clarified that whether data breaches are preponderantly insider attacks or outsider attacks depends on your definition of insider. If "insider" means "on the payroll," then insider attacks are not the most important issue. If, however, the term "insider" is expanded to include individuals who are employees of the firm's partners with access to the firm's data, then the majority of data losses are the result of insider attacks.[163]

In the civil sector, many firms conclude that dealing with cyber intrusions is simply a cost of doing

162 Daniel E. Greer, Jr., "Cybersecurity and National Policy," *Harvard National Security Journal*, 1, 2011, p. 210.

163 Ibid.

business, especially given that effective defenses against all forms of attack appear both impractical and very costly. This cost is matched against the cost of dealing with steady-state cyber intrusions. When such comparisons are made, a firm's Chief Financial Officer typically concludes that it is a waste of money to do more than provide a minimum level of cyber security. When a cyber attack or intrusion occurs, the firm simply works to recover as quickly as possible.[164] This approach may in fact be the most cost-effective strategy in dealing with the threat of "routine" cyber war operations (e.g., cyber crime, cyber commerce raiding, cyber espionage). In the case of a "black swan" catastrophic attack, however, it may fail dramatically.

THE PROBLEM OF ATTRIBUTION

Given that cyber warfare is, like nuclear warfare, offense-dominant, there may be an inclination to assume that the best way to deter an attack is

164 Andress et al., *Cyber Warfare*, p. 23. Yet this often destroys evidence necessary to determine how the systems were compromised in the first place; if forensics are not completed before the system is brought back on line, it may be impossible to determine what defenses need to be put in place to prevent the penetration from recurring. Thus an important element of defense is to have a backup system that can operate while the forensic effort proceeds to completion.

through the threat of retaliation. During the Cold War, for example, the United States and the Soviet Union relied on the threat of massive nuclear retaliation to deter large-scale nuclear attacks on their homelands. To be effective, a strategy of deterrence through punishment requires that the prospective attacker believe that he can be accurately identified by his target, that the target of the attack has both the capability and the will to retaliate, and that the costs incurred through a retaliatory attack (be it in the form of a cyber strike or more traditional military action) will exceed the benefits to be derived from the cyber attack.

This aspect of deterrence through retaliation—the need for accurate attribution—has existed until now with respect to nuclear attack. During the Cold War the United States and the Soviet Union deployed space-based sensors to watch the other side's bomber bases and land-based missile forces. In cyber space, however, the ability to promptly attribute the source of a cyber attack is almost certain to be far more problematic. As former deputy defense secretary William Lynn stated, "[T]raditional Cold War

deterrence models of assured retaliation do not apply to cyberspace, where it is difficult and time consuming to identify an attack's perpetrator."[165] The Internet is an ideal platform for conducting cyber attacks under cover of anonymity (i.e., we don't know who you are) or misdirection (i.e., we think you are someone you are not). Discriminating between attackers and divining an individual attacker's intentions can also be very difficult.

Cyber attacks occur very rapidly; consequently, they must be identified promptly to mitigate the damage that can be done to the targeted system. Intrusion Detection Systems provide some assistance here.[166] They work in part by detecting patterns of attack by a particular attacker. To perform effectively, however, IDS require that the attacker undertake multiple attempts to access the target. Thus, these efforts are unlikely to prove effective in circumstances where the intrusion is a single event. Put another way, employing IDS is most likely to be effective against DDoS attacks owing to the

165 Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," p. 99.

166 Jay P. Kesan and Carol M. Hayes, *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academics Press, 2010), pp. 330-331.

repetitive character of such attacks.[167] Detecting an attack is important since, once detected, tracing the attack to its origins can be accomplished in a matter of seconds through some form of traceroute. While traceroute is typically used to ensure that data is transmitted effectively through the Internet, similar technology can be used to identify the source of an attack. Traceroute technology employed in this manner is often referred to as traceback.[168]

This hardly solves the matter of attribution, however, as the attacker might be spoofing (where the attacker attempts to deceive the target as to the true source of the attack) his internet protocol[169] address in order to evade accurate attribution. Fortunately, IDS provides additional information that may be able to determine if the attack point of origin identified by traceback is inaccurate due to IP spoofing. This knowledge could prevent the defender from counterstriking an incorrect IP address, while also helping to locate the actual attack source. Yet even

167 Ibid., p. 332.

168 Ibid., p. 331.

169 Internet Protocol is the primary network protocol used on the Internet and supports unique addressing for computers on a network. Data on an Internet Protocol network is organized into *packets*, each containing a header (providing information about the packet's source and destination) as well as other information and the message itself.

if the IP address can be accurately determined, it does not constitute proof that a particular state or non-state entity is behind the attacks. Unless the target of the attack is observing the network when an attack occurs and sees it coming (and sometimes not even then), the defender may not be able to provide prompt attribution of an attack. For example, forensics may be able to trace the attack and identify the kind of keyboard used to initiate the attack (e.g., Arabic, Cyrillic, etc.), but that does not confirm that the attacker was of a particular nationality, let alone that he was acting on behalf of a government.[170]

A state (or even a non-state entity) seeking to execute a cyber attack whose objective is to inflict catastrophic damage on its target may seek to maintain anonymity. States engaging in such attacks could seek to develop and employ proxies. For example, computer systems in China appear to be used as an intermediary in cyber attacks. Although a particular computer system in China can seem to be the actual source of the attack, this may not be the case, as it is relatively easy to compromise a system and use it

170 Clarke et al., *Cyber War*, p. 214.

as a proxy to attack another target. If an attacker is able to develop several layers of proxies, particularly if each is located in a different geographical area, the attacker has a form of layered defense against efforts by the defender to attribute the source of the attacks. Once again, even if the source can be determined, it does not prove that the individuals controlling the source were acting on behalf of a particular government or non-state entity.

The case of the Conficker worm shows just how difficult both computer network defense and attribution can be. Conficker has infected millions of computer systems since its release in 2008. Despite the efforts of governments and private sector cyber sleuths, the command link between Conficker and its controllers remains unbroken.[171] Fortunately it does not appear to carry a malicious payload. But what if it did? The damage could be extensive. For those contemplating cyber defenses, the inability to either break the command link (which would reduce confidence that an attack would be successful) or identify its source (which would increase the

171 Bowden, "The Enemy Within."

chances of effective retaliation) would seem to make a strategy rooted in deterrence a risky proposition.

Making matters more difficult, even if an intrusion is detected and the target has high confidence regarding its source, it may not be possible to differentiate between an intelligence operation designed to obtain information and a cyber attack designed to inflict damage (e.g., corrupt or destroy data, substitute code, etc.).[172] Is an attempt to penetrate a computer system intended by those who launched it part of a reconnaissance effort to map the network, steal or corrupt data, take over the network, or destroy it? Mounting an effective defense against a cyber intrusion, limiting the damage from such an intrusion, or avoiding mischaracterizing an intelligence operation as an attack depends on the ability to answer these questions almost instantaneously at the time the cyber penetration occurs.[173] To provide some context, the demands placed on cyber defenses regarding defense timelines make those associated with intercepting a

172 Keith B. Alexander, testimony before the House Armed Services Committee, September 23, 2010, p. 5.

173 In cases where data has to be "exfiltrated" (that is, it has to travel back to the perpetrator), attacks are also more readily traceable. But this is not likely to be the case with respect to a cyber attack whose purpose is to inflict catastrophic destruction, rather than wage a cyber form of economic warfare or commerce raiding.

ballistic missile warhead traveling 10,000 miles per hour seem almost leisurely by comparison.

To be sure, a state contemplating a cyber attack against its adversary for the purpose of inducing catastrophic consequences would not likely conduct the attack as a "bolt from the blue." If a massive cyber attack occurred during a period of heightened tension between two states, this might increase the defender's confidence in its attribution efforts, particularly if its forensics efforts point to the rival state. *Yet this could also be the perfect time for a third party to route an attack through one of the two states in an effort to trigger a catalytic war.* Or it might be that one (or both) of the two states employs non-state proxy "cyber patriots" or terrorist organizations to both conduct the attacks and claim responsibility for them as a way of creating plausible deniability for itself and presenting its adversary with no real targets against which to retaliate.

Confidence in one's efforts at attribution might be increased if the cyber attacks coincided with other forms of military action, such as traditional military engagements employing kinetic weapons. But

one cannot rule out the prospect of a third party exploiting the situation to create an advantage for its preferred belligerent by conducting a cyber attack on its rival. To restate: assume State A and State B are at war but have not engaged in cyber attacks. State C has an interest in State B's defeat, and so has an incentive to execute a major cyber attack against State B to enhance State A's prospects of defeating State B.[174]

There also remains the challenge of attribution where attacks are being executed remotely through thousands (or even millions) of compromised computers in a botnet. One possible way of meeting this challenge involves developing and fielding collaborative intrusion detection systems (CIDS).[175] Efforts to develop such a defense are now under way.

There is also the matter of establishing a "standard of proof" with respect to attribution. How confident would the target of an attack have to be that it had correctly identified an attacker in order to retaliate against the (supposed) source? When confronted

174 One could plausibly substitute the word "non-state entity" for the word "state," particularly in the case of State C.

175 Kesan et al., *Proceedings of a Workshop on Deterring CyberAttacks*, p. 331.

with identifying attribution in the wake of a "strategic" cyber attack (i.e., an attack intended to inflict catastrophic levels of destruction), owing to the risks of undertaking a massive counterstrike against the wrong enemy (i.e., one that is assumed to have the ability to conduct a catastrophic attack) the standard of proof (reliability) in assigning attribution may be substantially higher than in other forms of cyber activity (e.g., cyber commerce raiding, cyber crime, cyber espionage).

For decision-makers in a state that is subjected to such an attack, the problem is likely to be complicated further, as public pressure for the victim state's government to respond both forcefully and promptly will almost certainly be great. Yet in many instances a significant amount of time will likely be required to enable forensics efforts to make as accurate an assessment as possible regarding the attack's source, further exacerbating the problem confronting the victim state's decision-makers. Moreover, such efforts are typically of greater value

in determining the attacker's capabilities than in determining attribution.[176]

In summary, attribution of a sophisticated attack is likely to be very difficult to prove from a technical standpoint. It may be possible for other forms of intelligence, particularly human intelligence (HUMINT) or signals intelligence (SIGINT), when combined with cyber forensics efforts, to provide information that conclusively leads to the true source of the attack. But again, the result is hardly assured, nor is such information likely to be available promptly. As General Alexander observed, attribution in cyberspace is, and will for the foreseeable future likely remain, "costly and comparatively rare."[177]

Given the difficulties associated with attributing the source of cyber attacks, a strategy to address the threat of catastrophic cyber attack whose central pillar is deterrence through the threat of retaliation seems fraught with danger. The difficulties associated with providing high-confidence attribution are likely to embolden risk-tolerant enemies. History

176 W. Earl Boebert, *Proceedings of a Workshop on Deterring Cyberattacks*: *Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010), p. 43.

177 Keith B. Alexander, testimony before the House Armed Services Committee, September 23, 2010, p. 4.

offers all too many examples of leaders who took what many considered to be high-risk "irrational" actions, from Adolf Hitler's declaration of war on the United States to Saddam Hussein's willingness to take on a U.S.-led global coalition in the First Gulf War. What acts of aggression might such leaders undertake if they believed they had a significant chance of escaping responsibility for them? Such individuals might be especially attracted to the idea of triggering a catalytic war through cyber attacks, one that could see catastrophic damage as a second-order effect.[178] Such a strategy also fails to address the challenge posed by non-state actors, such as terrorist organizations and other radical movements that may have nothing of sufficient value against which to retaliate. Ironically, such groups may "solve" the attribution

178 As an example, consider the September 2007 Israeli attack on the Syrian nuclear reactor under construction at Deir ez-Zor. There are reports that the Syrian "state-of-the-art" air defense system failed to identify the attacking Israeli aircraft—none of which were stealth aircraft—because the Israelis had introduced some kind of malware into the system. In effect, the malware adjusted the data provided by the system, presenting Syrian observers with a picture of an empty sky when in fact Israeli aircraft were operating in Syrian air space. See David Fulghum, "Why Syria's Air Defenses Failed to Detect Israelis," *Aviation Week*, October 3, 2007, available at http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckScript=blogScript&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog%3a27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3a2710d024-5eda-416c-b117-ae6d649146cd, accessed on January 10, 2012; and Sally Adee, "The Hunt for the Kill Switch," *ieee Spectrum*, May 2008, available at http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0, accessed on January 10, 2012.

problem by anxiously seeking recognition of their responsibility for a mass cyber attack.[179]

THE POTENTIAL FOR CATASTROPHIC FAILURE

Cyber security executives from critical infrastructure firms, both in the United States and overseas, state that their networks are being subjected to repeated cyber attacks, often from advanced persistent threats.[180] The attacks range from large-scale DDoS attacks seeking to shut down systems to subtle efforts to penetrate networks through spear phishing. Experts in China have published theoretical papers on how cascading failures in the U.S. power grid might be generated.[181]

---

179 The problem for the victim of such a cyber attack, however, is compounded if multiple non-state groups claim responsibility for the attack (i.e., the "Spartacus Effect"). Should this situation occur, the problem of attribution would once again be confronted. That said, it does appear likely that the true attacker could provide "proof" by revealing to its victim certain aspects of the cyber payload that only its originator would have knowledge of.

180 Steward Baker, Shaun Waterman, and George Ivanov, "In the Crossfire: Critical Infrastructure in the Age of Cyber War," McAfee, 2010, pp. 1, 3, 11, available at http://iom.invensys.com/EN/pdfLibrary/McAfee/WP_McAfee_In_The_Crossfire_03-10.pdf, accessed on January 28, 2012. McAfee surveyed 600 IT and cyber security executives in the U.S. and abroad who are involved in protecting critical infrastructure. See also "Advanced Threats: The New World Order," RSA APT Summit Findings, October 2011, available at http://www.rsa.com/products/sms/sb/11545_RSAAPTs_NewWorldOrder_FindingsWP.pdf, accessed on April 17, 2012.

181 Jian-Wei Wang and Li-Li Rong, "Cascade-based attack vulnerability on the US power grid," *Safety Science*, 47, 2009, pp. 1332-1336; Wenkai Wang, Qiao Cai, Yan Sun, and Haibo He, "Risk-Aware Attacks and Catastrophic Cascading Failures in U.S. Power Grid," *IEEE GLOBECOM 2011, Proceedings,* 2011, pp. 1-6; and Siddharth Sridhar, Manimaran Govindrasu, and Chen-Chung Liu, "Risk Analysis of Coordinated Cyber Attacks on Power Grid," in A. Chakrabortty and M.D. Ili´c, eds., *Control and Optimization Methods for Electric Smart Grids*, *Power Electronics and Power Systems* 3, pp. 275-294. See also John Markoff and David Barboza, "Academic Paper in China Sets Off Alarms in U.S.," *New York Times*, March 20, 2010, available at http://www.nytimes.com/2010/03/21/world/asia/21grid.html?_r=1, accessed on April 17, 2012.

The cost of dealing with these attacks is substantial. Moreover, the vast majority of these executives believe that their sector would be the target of a successful major cyber attack by 2015.[182] Vice Admiral (Retired) Mike McConnell, former Director of National Intelligence, seconded these concerns when he concluded, "the most critical threats of our time, with the lowest barriers to entry, are those to our cyber infrastructure."[183]

Given the onset of cloud computing that offers firms the ability to lease server infrastructure and software, the situation may improve—or get worse. The views of one cyber security expert sum the situation up nicely:

> [C]loud computing scares the hell out of me. Not because I know of any particular specific problem inherent in it, but because, historically speaking, every time we have moved into a new area we have failed to appreciate what new potential for attacks has been created. We are creating yet more complex systems, and yet more systems that depend for their value on providing services to loosely coupled or loosely authenticated other systems.[184]

182 Baker et al., "In the Crossfire," pp. 1, 3, 11.

183 McConnell, "Cyber Insecurities: The 21st Century Threatscape," p. 27.

184 Baker et al., "In the Crossfire," p. 36.

To date, the United States has been unwilling to undertake the large-scale efforts needed to reduce substantially single point of failure systems, or to limit the use of systems that promote monocultures and thus can trigger a cascading failure. There appears to be little, if any, thought given in the private sector to the risks associated with relying on global supply chains (i.e., foreign states) for IT equipment, to include sensitive hardware and software components. While some firms have established internal "red teams" (i.e., cyber security staff that function as attackers or intruders) that mimic enemy efforts to penetrate their systems (e.g., by spear phishing), such efforts appear to be the exception rather than the rule. Among a group of 600 critical infrastructure cyber security experts surveyed, almost a third believed their sector was either "not at all prepared" or "not very well prepared" to deal with a cyber attack from an advanced persistent threat.[185]

These observations are admittedly somewhat speculative. Given the secrecy surrounding cyber

185 Ibid., p. 16.

operations it is unclear to what extent either the U.S. Government or private sector firms have been willing and able to erect effective layered defenses. Washington has also clearly been reluctant to take measures to improve warning and defense against cyber attacks if those measures could be construed as undermining privacy rights.[186] Even if such defenses were in place, it is unlikely they would be totally effective. Moreover, even if they were airtight, these defenses would not present an answer to the threats associated with the global supply chain and insiders.

Of course attitudes might change following a catastrophic cyber attack. Among the potential targets of such an attack are the power grid, transportation sector, financial sector, energy infrastructure, public health system, and water purification and distribution systems. What follows is a brief discussion of two sectors, the power grid and the financial sector. The objective here is not to be comprehensive, but rather to give the reader a general sense of critical

186 There appears to be a direct link between individual privacy and defense against cyber attacks. Ed Giorgio, then chief cryptanalyst for the NSA, stated that "In our line of work, security and privacy are a zero sum game." Another cyber expert echoed Giorgio's observation when he concluded, "[I]f, the tariff of security is paid, it will be paid in the coin of privacy." For both quotes, see Daniel E. Geer, Jr., "Cybersecurity and National Policy," *Harvard Law School National Security Journal*, 2011, p. 1, available at http://harvardnsj.org/2011/01/cybersecurity-and-national-policy/, accessed on January 10, 2012.

infrastructure vulnerabilities, especially those that pertain to the United States. This also conforms to what is possible. None of the sectors named above, nor any other part of the nation's critical national infrastructure provide details on their inner workings lest they be exploited by enemies seeking to attack them.

The Power Grid

A World of Power Disruptions?

Most Americans are used to the occasional power outage that lasts a few moments or perhaps even a few hours. And many have endured the loss of electric power in their homes for several days following a rare natural disaster (e.g., hurricane, blizzard, ice storm); few have been subjected to power outages lasting more than two weeks, or frequent (i.e., six or more a year) outages that last longer than several days. Moreover, most of these outages are localized, with some communities losing power while others nearby maintain power. In the event of localized protracted outages, those affected can migrate fairly easily to areas with power to obtain food and

shelter. In the event of a protracted and widespread outage, this would not be practical for many people.

According to one survey, over half of the attacks being conducted against the energy/power and oil/gas sectors target these firms' SCADA control systems.[187] The Conficker worm raised eyebrows when it managed to work its way into some of these systems.[188]

Without electric power the United States would quickly find itself in many ways back in the 19th century, with the attendant consequences for its citizens' well-being.[189] At a more modest level, if the U.S. power grid were subject to frequent, extended disruptions it would likely result in major and enduring costs incurred to cope with the outages. For example, the loss of refrigeration could risk the

187 In 2007 the U.S. Government's Idaho National Laboratories conducted a test that found hackers were able to compromise the SCADA control system that ran a large diesel generator, causing it to physically self-destruct. Douglas Birch, "Cyber Attacks on Utilities, Industries Rise," *Boston Globe*, September 29, 2011, available at http://www.boston.com/news/nation/washington/articles/2011/09/29/us_cyber_attacks_on_utilities_industries_rise/, accessed on January 31, 2012. In 2011 there were reports that hackers had shut down a water utility's pump in central Illinois by powering it on and off repeatedly until it burned out. Jim Finkle, "US Probes Cyber Attack on Illinois Water System," *Reuters*, November 18, 2011, available at http://www.reuters.com/article/2011/11/19/cybersecurity-attack-idUSN1E7AH1QU20111119?feedType=RSS&feedName=everything&virtualBrandChannel=11563, accessed on April 19, 2012; and Jim Finkle, "Foreign cyber attack on Illinois water utility," *The Daily Caller*, November 18, 2011, available at http://dailycaller.com/2011/11/19/foreign-cyber-attack-on-illinois-water-utility/, accessed on January 31, 2012.

188 Baker et al., "In the Crossfire," pp. 9, 22-23, Over three-quarters of the executives surveyed whose firms employed SCADA systems had them connected to an open network (e.g., the Internet). As SCADA systems typically combine hardware and software, replacing them can be a complex and expensive undertaking.

189 Of course, it can be argued that were the United States to divorce itself entirely from the Internet it would find itself back in the late 1980s. While hardly as dire a situation as the late 19th century, this would still represent "extreme misfortune" in terms of economic loss and a corresponding decline in its citizens' standard of living and quality of life.

large-scale loss of perishable foodstuffs. Pumps required for water and sanitation systems could be disabled. Depending upon the season, the loss of heating and cooling systems could cause significant health problems.

The prospect of frequent power interruptions becoming a way of life could impose major, enduring costs on the United States. Assuming they can afford it, individuals may purchase backup generators to ensure the food in their refrigerators does not spoil, the pipes in their homes do not freeze, etc. Some firms in the food business ranging from food suppliers (e.g., supermarkets) to restaurants may require backup power on a far greater scale than is currently the case. Backup power systems would likely be needed to regulate traffic in the absence of traffic lights as would the ability to operate trains powered by electricity. Service stations would need to install backup systems to enable their gas pumps to function, lest automotive transportation break down. Businesses that rely on computers and the Internet might also install backup power systems to continue operating during periods of power outage. Water

and sewage systems would need to install backup generators or, if they have them, replace them on a much more frequent basis than is now the case. Power companies would likely take their SCADA systems off the Internet; however, this would not solve the problems associated with insider threats or reliance on a global supply chain.

A Vulnerable Grid

Could a cyber attack take the United States, or major parts of it, off the electric grid for significant periods of time? While it is not possible to provide a definitive answer, there is sufficient evidence to justify concern that such an event could occur.

Initially U.S. power grid control systems (i.e., SCADA systems) were on closed networks that were not connected to the Internet. Over time, however, the electric industry began relying on SCADA systems to improve the efficiency and performance of their systems. As it is cheaper to maintain an open network than a closed one, firms opted to move to open networks. Access to the Internet, with its

attendant benefits and vulnerabilities, became essential for operations.[190]

In addition to penetrating power companies via the Internet, hackers can compromise SCADA systems by exploiting outdated modems used for maintenance purposes, or by exploiting wireless access points—jumping the "air gap." Again, irrespective of being on an open or closed network, the problems of supply chain security and insider threats remain. Finally, power companies may buy and trade power among one another, creating the prospect that hackers breaching the defenses of one firm will have effectively penetrated all its partners as well.[191]

The U.S. power grid's vulnerability is heightened by two additional factors. First, most grid asset owners and operators have been historically resistant to report cyber attacks against their networks or to make the necessary investments to upgrade and secure their networks.[192] Second, the U.S. power grid is highly centralized; the power grid serving the contiguous forty-eight states is composed

190 Clarke et al., *Cyber War*, pp. 98-99.

191 Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," p. 66.

192 Carr et al., *Project Grey Goose*, p. 3.

of three distinct power grids, or "interconnections"—the Eastern Interconnection, the Western Interconnection, and the Electric Reliability Council of Texas Interconnection.[193] These interconnections provide power to the continental United States, Canada, and a small part of Mexico. The combination of centralized grids and a lack of emphasis on defensive measures could make the power grid more vulnerable to cascading failures, as have been triggered by other events in the past. As roughly 90 percent of the Defense Department's most critical assets are entirely dependent on the bulk power grid, there is the potential for a "Cyber Pearl Harbor" to result from a successful attack on the grid.[194]

A recent case points out just how vulnerable the grid may be. In 2008 a power company hired a cyber security firm to test the security of the network it employs to oversee its power grid. The cyber security team took only a day to organize its cyber tools before launching its attack. The penetration team monitored SCADA user groups, harvesting the email addresses of people working at the targeted

193 Ibid., p. 4.

194 Ibid., p. 3.

power company. It then sent the workers an email describing the company's intention to reduce their benefits along with a link to an Internet site where they could obtain more information. When the employees clicked on the link, they were directed to an Internet server set up by the penetration team. The employees' machines displayed an error message; however, the Internet server downloaded malware enabling the team to take command of the machines in less than one day.[195]

The situation may become worse before it gets better. In particular, the recent move by the United States to develop a "smart grid" could increase the United States' vulnerability to cyber attacks on its electric power infrastructure.[196] The U.S. Department of Energy (DoE) is working to build security into the smart grid, but the challenge is very complex.[197]

195 Tim Greene, "Experts hack power grid in no time," *Network World*, April 9, 2008, available at http://www.networkworld.com/news/2008/040908-rsa-hack-power-grid.html, accessed on January 29, 2012. The SCADA systems targeted are inherently insecure as they run on standard operating systems on standard server hardware, thereby subjecting them to those systems' vulnerabilities. Although many power companies are aware of the problem, they have typically preferred to avoid incurring the risk of interrupting service, which may occur if they attempt to install software upgrades to improve security.

196 Carr et al., *Project Grey Goose*, p. 3.

197 Andress et al., *Cyber Warfare*, p. 24.

A Growing Cyber Threat?

Reports in the open source literature indicate that the power grid has been targeted by cyber operations. In 2003 the Slammer worm temporarily took a U.S. nuclear power plant's safety monitoring system offline.[198] That same year the Blaster Worm allegedly was associated with a massive blackout that occurred in the eastern United States.[199]

More recently, in 2008 the CIA reported that multiple cities outside the United States had their electrical power shut off by hackers. The report was short on details, apparently owing to security concerns, but stated that the attacks came through the Internet.[200]

Such attacks may not be the sole province of nation-states. For example, computers and manuals seized in al Qaeda training camps contained large amounts of SCADA information related to dams and other critical infrastructure.[201] One could imagine other non-state entities whose capabilities—both in

198 Clarke et al., *Cyber War*, p. 99. It is not clear, however, that this was a deliberate attempt to attack either the nuclear power plant or the U.S. power grid. I am indebted to Herbert Lin for this observation.

199 Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," p. 65. Again, it is not clear that those employing the worm sought to attack the power grid.

200 Ibid. In at least one instance the blackout was found to have been caused by factors other than a cyber attack.

201 Ibid.

terms of intellectual and financial resources—are likely to be far greater than those of al Qaeda.

In October 2009 Project Grey Goose was established to determine whether there had been any successful hacker attacks against the power grid, both in the United States and in other countries. The project concluded that state and/or non-state actors from a number of countries, most likely China, Russia, and the Commonwealth of Independent States, are almost certainly targeting and penetrating energy provider networks as well as the networks of other critical infrastructures. Among their top priority targets are the United States, Brazil, Russia, and the European Union.[202]

The attacks have apparently been occurring at low levels for at least a decade. It has not been possible to provide definitive attribution as to who was behind the attacks. There is, however, considerable circumstantial evidence that the states cited above are behind a great many of them. For example, following the death of a People's Liberation Army pilot in a collision with a U.S. military aircraft on April 1, 2001, thousands

202 Carr et al., *Project Grey Goose*, p. 2.

of Chinese hackers launched a series of concentrated attacks against U.S. websites in what the *New York Times* dubbed "The First World Hacker War."[203]

The attacks peaked on May 7, coincidentally the two-year anniversary of the accidental U.S. bombing of the Chinese embassy in Belgrade during the 1999 Balkan War (also known as Operation Allied Force). That same day California experienced rolling blackouts over two days, affecting some 400,000 customers.[204] An investigation by the California Independent System Operator (CAL ISO) revealed that hackers had gained access to two Solaris web servers that supported CAL ISO's network and maintained access from April 25 until May 12, the last day of large-scale attacks. Nevertheless, CAL ISO claimed that this breach of its cyber defenses was not related to the blackout. Despite these claims, press reports from the *Los Angeles Times* claimed access to inside information from CAL ISO that concluded that the cyber penetration came close to producing a "catastrophic breach" of the system. The

203 Craig S. Smith, "May 6-12; The First World Hacker War," *New York Times*, May 13, 2001, available at http://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html, accessed on January 10, 2012.

204 Carr et al., *Project Grey Goose*, p. 7.

cyber attack on CAL ISO was traced to Guangdong province in China.[205]

Project Grey Goose also concluded that network attacks against the bulk power grid will almost certainly escalate steadily in frequency and sophistication over time due in part to international emphasis among the G20 nations on smart grid research, collaborative energy development projects, and the new opportunities these efforts are likely to create for acts of cyber espionage.[206]

The Financial System

Another key part of the U.S. critical infrastructure that is heavily dependent upon computer systems and networks is the financial system. Could the U.S. and (by extension) the global financial system be subjected to a catastrophic cyber attack? The stakes involved and the risks associated with the compromise of a financial computer system or network are potentially profound. Even more than other parts of the critical infrastructure, like the power grid and

205 Ibid., p. 12.

206 Ibid., p. 2.

the transportation system (e.g., air traffic control systems and train routing systems), the financial system's effective functioning depends upon the confidence of people. One Wall Street CEO summed it up well: "It is confidence in the data, not the gold bullion in the basement of the New York Fed, that makes the world financial markets work."[207]

Were people to lose confidence in the financial system's ability to keep accurate track of their funds, prevent their funds from being siphoned off, or engage in unauthorized transactions using their funds, the system could suffer a catastrophic failure even in the absence of any significant physical damage. Depending on the severity of the losses incurred, the loss of confidence in the system could be both widespread and enduring. Given the stakes involved and the risks of failure, it seems likely that the financial sector devotes a substantial amount of resources to defending its computer systems and networks from compromise or attack, to include maintaining entire backup systems on networks separate from those that are in active use. Whether these activities are

207 Clarke et al., *Cyber War*, p. 240.

sufficient to defend against or deter a determined attack is unclear, especially considering the challenge associated with the lack of security in global supply chains and the threat of an insider attack.

ADVANCES IN CYBER WEAPONS: CONFICKER AND STUXNET

Recent developments in cyber weapons have only served to increase concerns over the vulnerability of critical infrastructure. Two of the potentially most powerful cyber weapons, called Conficker and Stuxnet, are summarized below to provide the reader with a sense of the competition as reported in open-source documents.

Conficker

The Conficker worm was introduced in November 2008. A self-replicating program, Conficker quickly spread around the world by exploiting networks or computer systems that utilized the Microsoft Windows operating systems monoculture and that failed to keep their security up to date by downloading

the latest security patches.[208] Conficker could infect machines via the Internet (or a closed Intranet) or achieve penetration via a compromised USB device. After penetrating via the Internet or Intranet to gain access, Conficker patched the "hole" (at Port 445) through which it came.[209] This enabled the worm to avoid competing for access with other malware seeking to exploit the vulnerability for their own purposes. Through this process Conficker's controllers established a massive botnet estimated to link upwards of 6-7 million computers.[210]

The Conficker botnet is a powerful cyber weapon with the potential, theoretically, to inflict prompt, catastrophic destruction. Working together under the command of a single controller, the millions of Conficker-controlled computers would represent an enormous amount of computing power. Aside from its ability to execute massive DDoS attacks, the Conficker botnet could crack sophisticated codes,

208 Hathaway, *Strategic Advantage*, p. 4.

209 Bowden, "The Enemy Within."

210 Ibid., p. 3.

perhaps enabling its controller to breach, compromise, and even destroy protected databases.[211]

But having amassed a zombie army, its commanders did—nothing. Once it had established itself as described above, the worm did nothing more than call home periodically for instructions.[212] Given the threat posed by Conficker should it be activated, cyber security experts mobilized to control and defeat it.

In February 2009 an array of cyber security experts combined to form the Conficker Working Group.[213] Microsoft offered a $250,000 bounty for the arrest and conviction of the worm's creators.[214] Computer security experts soon created software that deleted the worm from millions of infected computers. Yet rather than concede defeat, Conficker's author(s) continued releasing new versions of the worm that

211 Ibid.

212 Ibid., p. 5.

213 Rodney Joffe, senior vice president and chief technologist of Neustar, led the group battling Conficker. The group called itself the Conficker Cabal. Joffe's firm, Neustar, provides a global trunk-line service for cell-phone companies. Simply put, Neustar keeps track of every single phone number and this enables it to know where to route calls so they end up in the right place. Almost every phone call being made in North America asks Neustar for directions in order to be completed. A botnet like Conficker could theoretically be used to shut down Neustar's system. Were this to happen, entire countries could be cut off from the telecommunications grid. To be sure, individuals with cell phones would still be connected to the telecom grid, but their calls could not be routed to their destination. Interestingly, when the Obama administration announced it would hire "a thousand" computer-security experts over the next three years, Joffe lamented the government's ignorance of the cyber competition, asserting "There aren't more than a few hundred people in the world who understand this stuff." Ibid.

214 Ibid., p. 10.

included enhanced code, much to the surprise of the experts who were working to combat it.

Reflecting the worm's potential power, by early 2009 Conficker B had invaded the United Kingdom's Defense Ministry; as CBS prepared a *60 Minutes* segment on the worm, its computers were struck.[215] A later version, Conficker C, introduced "peer-to-peer" communications, in which computers can send information directly to one another while circumventing a centralized server.[216] Now a computer that had been infected by Conficker could (and did) spread the worm directly to every machine with which it interacted. Instructions no longer needed to be routed through servers to individual computers via a command center; they could now be sent from computer to computer. This innovation reduced the ability of cyber security experts to determine how many computers were infected, since

215 Ibid.

216 Ibid., p. 12. See also Phillip Porras, Hassen Saidi, and Vinod Yegneswaran, "Conficker C P2P Protocol and Implementation," SRI International Technical Report, September 21, 2009, available at http://mtc.sri.com/Conficker/P2P/, accessed on January 21, 2012. Put another way, a peer-to-peer network exists when computers are interconnected as a network, but no computer occupies a privileged position. Every computer can communicate with all the other machines on the network, with each computer generally storing its own files and running its own applications. In a sense, each computer can function as a server and a client of the other computers (which can also function as servers). The peer-to-peer network is ideal for sharing files among computers directly. Napster, the music file-sharing service, was a pioneer in peer-to-peer networking.

Conficker no longer needed to contact its master(s) directly.[217]

By the spring of 2009 there were already multiple versions of Conficker in cyber space. One of the newer and more sophisticated variants, Conficker E, self-destructed in May of 2009. As it disappeared, like the Cheshire cat in *Alice and Wonderland*, it took the control connections to a large number of botnet nodes with it.[218]

Given its seemingly benign disappearance, what was the purpose behind Conficker? No one quite knows. Some speculate that it was created as a proof of concept for a cyber weapon, and that its deployment enabled its master(s) to conduct the equivalent of a field test to confirm that a worm could be embedded and spread quickly, and that even after being detected it could sustain its command and control links despite efforts to break them.[219] Interestingly, other variants of Conficker are still embedded in

217 Ibid., p. 12.

218 Andress et al., *Cyber Warfare*, pp. 203-204.

219 Ibid., p. 204.

computers around the world: the Conficker botnet army is still growing.[220]

Perhaps even more worrisome is that few cyber experts believe Conficker is the product of a state's cyber weapon program.[221] This is because the worm spreads indiscriminately, rather than focusing on a specific target set. Their logic is that a state would want its cyber weapons to be discriminant—to attack only the particular set of targets associated with a specific enemy. Conficker's behavior appears more associated with a desire to undertake an act of wanton (or unfocused) infection with no other end in mind.

Moreover, a nation seeking to create a botnet weapon is unlikely to create one as brazen as Conficker, whose creators seem to have enjoyed the back-and-forth game with the cyber security forces trying to defang it. The prospect of weapons like Conficker being possessed by a radical non-state entity poses a significant potential threat to the security of states.

---

220 For a summary of the efforts to bring Conficker under control, see *Conficker Working Group: Lessons Learned*, June 2010, available at http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf, accessed on April 17, 2012.

221 Bowden, "The Enemy Within," pp. 13-14. China is the nation most often suspected in cyber attacks. Ironically, given the number of computers in that country operating on pirated copies of Microsoft's operating system, there may be more Conficker-infected computers in China than anywhere else.

In summary, Conficker's creators have figured out how to establish a large botnet and maintain its command-and-control links despite the efforts of cyber security experts in both the public and private sectors. Having field tested Conficker, its author(s) can use the knowledge gained to craft a more dangerous worm for their own use, or perhaps to sell it to a radical group bent on nothing more than causing the maximum degree of destruction possible. Of course, there would be nothing to stop them from selling such weapons to states or, perhaps more likely, offering to employ them for a state while serving as its proxy.

Stuxnet: Cyber War, Western Style?

Perhaps the most impressive piece of malware that has come into the public eye is not the product of either organized cyber crime or autocratic regimes like those in China and Russia, but most likely the product of one of the western democracies or Israel. Discovered in 2010, the Stuxnet computer virus that penetrated Iran's nuclear weapons program took control of key SCADA systems that directed

centrifuges engaged in enriching uranium. Once in control, the virus directed the centrifuges to operate at unsafe speeds. This resulted in their physical damage, evidently in some cases to the point of destruction, requiring costly and time-consuming repairs, thereby delaying Iran's uranium enrichment efforts.

Stuxnet is remarkable on several levels. First, it is a highly sophisticated virus. In a sense, it is the first "precision-guided" cyber weapon in that it focused on a specific target. As in the case of smart munitions versus "dumb bombs," the level of resources involved in Stuxnet's development was far greater than that associated with "garden variety" viruses. Stuxnet's "precision guidance" went beyond targeting a particular type of control system; it was also designed to attack a particular kind of facility.[222]

Experts determined that the virus was designed to target Simatic WinCC Step7 software, an industrial control system made by the German conglomerate Siemens.[223] The controllers, or SCADA systems,

222 Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, p. 4, available at http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/, accessed on January 10, 2012.

223 Ibid.

drive and regulate the motors, valves, and switches in a wide range of industrial applications, to include food factories, automobile assembly lines, gas pipelines, electric utilities, and water treatment plants

The attackers wanted to spread their virus, but in an unusual way. Unlike most malware that employs email or malicious websites to infect computer systems *en masse*, none of Stuxnet's exploits leveraged the Internet. They all spread via local area networks, apparently through infected USB thumb drives that were corrupted by a single USB stick smuggled into a closed Iranian facility and onto a closed computer network.[224]

When the Stuxnet-infected USB stick was inserted into a computer, the exploit code surreptitiously delivered a large, partially encrypted file onto the computer. What particularly impressed many cyber security experts, however, was how Stuxnet hid its functions through a "ghost file" that was not stored on the computer's hard drive, but rather in its memory as a "virtual" file. The virus reprogrammed the Windows interface between the operating system

224 Ibid., p. 9.

and the programs that ran on it so that when the computer tried to load a function from its hard drive library with the Stuxnet file name, the file was pulled from memory and not the hard drive. By placing the ghost file in the computer's random access memory rather than its hard drive, Stuxnet became more difficult to find, especially since the cyber security experts who examined Stuxnet had never seen this technique.[225]

Embedded in Stuxnet's code were files detailing the specific technical configuration of the facility it sought to attack. Those systems whose configurations were not a precise match remained unharmed. Stuxnet would simply move on to the next system until it found an appropriate match. By designing the virus in this way, its developers apparently intended to target closed systems isolated from the Internet. Also impressive was Stuxnet's "armament;" the virus contained no less than four zero-day exploits to insure that, if it penetrated the networks defenses, it would be able to seize control of the computer system.[226] One cyber security expert remarked, "To see

225 Ibid., p. 6.

226 Ibid., p. 9.

that somebody built such a sophisticated piece of malware—using four zero-day vulnerabilities, using two stolen certificates—to attack one single installation? That's unbelievable."[227]

The combination of skill and resources involved in creating Stuxnet (to include the intelligence effort associated with obtaining a clear picture of Iran's centrifuge computer network infrastructure) convinced experts that it had to be produced by an advanced persistent threat.[228] Given that Iran was the target suspicions immediately turned to the United States and Israel as the virus' likely creator(s).

CYBER WAR AND CATASTROPHIC DESTRUCTION: A FIRST CUT

What might we conclude based on open-source accounts regarding the development of cyber weapons and their prospects for inflicting prompt, catastrophic destruction? Might sophisticated "precision-guided" cyber weapons like the Stuxnet

227 Ibid., p. 14.

228 As one expert noted, "This is what nation states build if their only other option would be to go to war." Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare* (London: Chatham House, 2010), p. 20.

virus provide the means for a state to conduct an attack producing prompt, catastrophic destruction? Based on the information available in the open-source literature, it is theoretically possible that an array of logic bombs could be planted at key points throughout a state's critical infrastructure. But this would, among other things, require the attacker develop an accurate mapping of these systems, find a way to access closed networks separated from the Internet, and maintain a command and control link to insure that the logic bombs would "detonate" when ordered to do so. Achieving this level of accurate penetration and control is hardly a sure thing; indeed, it seems quite unlikely at the present time.

Some experts assert that with its discovery and elimination, Stuxnet has no value as the systems it might target can now be directed to scan for Stuxnet's presence and eliminate it, even if the virus manages to penetrate the system.[229] But this misses the point. Stuxnet was discovered only *after* it had initiated its attacks.

229 Zetter, "How Digital Detectives Deciphered Stuxnet," p. 22.

Perhaps even more worrisome, as Stuxnet was operating on a closed system (i.e., a computer network isolated from the Internet), the attackers could not maintain effective control over the weapon. Much like the lone B-52 bomber that had lost communications with its headquarters in the motion picture, *Dr. Strangelove*,[230] once it had penetrated the defenses of a closed network, Stuxnet was on its own. It attacked targets in accordance with instructions formulated before it was launched—instructions that would be difficult to change once the virus entered the closed system. If Stuxnet's attacks had generated unwanted second-order effects, there was no quick and effective way to stop it.

But much of the United States' (and many other countries') critical infrastructure is linked to the Internet, an *open system*. As the Conficker worm demonstrated, it is possible, apparently even for a non-state entity, to embed a cyber weapon on millions of systems *and maintain command and control links despite the best efforts of some of the best*

230 In *Dr. Strangelove*, a U.S. general orders an unauthorized nuclear-armed bomber strike against the Soviet Union. Eventually all of the bombers are recalled before they attack—all but one, which has lost its ability to communicate with its headquarters. Columbia Pictures, *Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb*, 1964.

public and private sector cyber security experts to break them. And as Stuxnet showed, it is also possible for a cyber weapon to physically damage and even destroy critical pieces of equipment. It thus appears plausible, at least in theory, for a state to produce a cyber arsenal comprising a wide variety of "designer" or "precision" cyber weapons, each crafted to usurp the many types of control systems employed in overseeing a target state's critical infrastructure, and embed these weapons with their controller counterparts. If Conficker provided a "proof of principle" with respect to an attacker's ability to maintain robust command and control links between the embedded cyber arsenal and its masters, then a mass coordinated attack on a nation's infrastructure producing prompt, catastrophic damage seems plausible.

That said, there are a number of big "ifs" at work here, even assuming cyber weapons can be embedded in their targets and command and control maintained. For one thing, the effects of a nuclear blast are fairly well understood, while the effects of a cyber weapon may not be. The wide range of

cyber weapons required to align properly with their targeted SCADA systems would likely raise doubts regarding how effective they would be when actually employed in an attack. To be sure, given that the SCADA systems employed in the private sector are generally available commercially, it should be possible to undertake tests of a particular cyber weapon's effects on such systems. This could reduce the uncertainty associated with the likely results of an attack, perhaps significantly. Yet it may be difficult to discern through this kind of testing the second-order effects of such attacks. For example, power grids are in some cases linked across international borders. Taking down an enemy's power grid may also knock out a neutral or even friendly country's power.

Then there is the matter of the target state's ability to recover from the attack. How quickly and completely could remediation occur? To what extent can this be known in advance? Answers to these questions could greatly influence an attacker's confidence in a cyber attack's ability to produce prompt, catastrophic destruction.

To return to our air power analogy, it may be that at present we are likely to find a massive cyber attack on an advanced state’s critical infrastructure achieves results more similar to those of the strategic bombing campaigns of World War II, rather than the prompt and catastrophic damage of a major nuclear attack.

CHAPTER 5 > ARE CYBER WEAPONS "STRATEGIC" WEAPONS?

This chapter addresses the issue of whether cyber weapons are "strategic" weapons in the sense that, if properly employed, they can trigger catastrophic destruction within a relatively short time span. At this point it may be useful to assess to what extent cyber weapons share qualities with nuclear weapons. The latter, since their inception, have occupied a unique position in warfare as clearly capable of producing catastrophic effects. To the extent that nuclear and cyber weapons have similar characteristics, they might be similar in terms of the effects they can produce. The discussion that follows finds that while nuclear and cyber weapons share some important characteristics, they are far more different than alike.

Two Offense-Dominant Regimes

One important quality that both nuclear and cyber weapons share is that the competition favors the offense. Put another way, given equal resources, the side that invests in offense has the advantage. With respect to the nuclear competition, the U.S. military, generally acknowledged to be the world's most technically sophisticated, has yet to develop an effective defense against nuclear ballistic missile attack despite over a half century of effort and hundreds of billions of dollars. Similarly, it appears that it is far less taxing to develop an offensive cyber capability than it is to defend against the various forms of cyber intrusion and attack. Were the case otherwise, cyber economic warfare, cyber crime, and cyber espionage would not be the problems they are. We might paraphrase the words of Stanley Baldwin in concluding that, as things stand today, while not all nuclear-armed ballistic missiles will get through, it seems likely many and even most of them will. Similarly, while every cyber weapon may not reach its target, it seems plausible that many and perhaps most of them will.

Defenses

While both the nuclear competition and the cyber competition are offense-dominant, the latter competition has a much more dynamic quality to it. A major difference between nuclear and cyber attacks is that unlike nuclear attacks, cyber warfare activities are highly vulnerable to physical effects. Once a major nuclear attack designed to produce catastrophic destruction is under way, especially in the case of nuclear weapons delivered by ballistic missiles, there is little in the way of defensive measures that can prevent the attack from succeeding. Missile defenses may be able to reduce the attacker's numbers at the margin, and passive defenses may place some limits on the damage wrought by the attack (again, at the margin), but such defenses can be overwhelmed far more easily—and cheaply—than they can be fielded.

This may not be the case with cyber attacks, at least not in the case of those that must be executed via the Internet. If the target severs its access to the Internet, or if power is cut-off even partially, the ability to deliver a cyber strike, let alone conduct a

cyber campaign, may be seriously compromised. To be sure, in such cases the cyber attacker may achieve something akin to a "mission kill" in that the defender's severed access to the Internet may prohibit his ability to perform key functions (e.g., financial transactions). Still, this is not an option open to those targeted by a nuclear attack.

Moreover, once the attacker's "exploits" are triggered, he may not be willing to risk that his victim will be able to identify the attack's source, or that the victim will retaliate against him even in the absence of effective attribution. In this case, the attacker will likely engage in vigorous efforts to block retaliatory attacks. These efforts may not succeed entirely, but could be effective enough to discourage such attacks or significantly limit their effects. For example, immediately after executing an attack, Beijing may disconnect the country from the global Internet.[231] The Chinese (or another enemy) may also prevent Cyber Command from launching retaliatory attacks by disabling portions of the U.S. Internet.[232]

---

231 Clarke et al., *Cyber War*, p. 146. Of course should China disconnect itself from the global Internet it would still be possible to conduct attacks from within China (e.g., by exploiting internal Internet connections, using "insiders" with access to key networks, etc.)

232 Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, April 8, 2009.

War and Peace

A key distinction between nuclear and cyber weapons concerns the line between war and peace. With regard to the former, perhaps the clearest signal that a state could give another that they are at war is to attack with a nuclear weapon. This is not at all the case with cyber warfare, where the line between war and peace is blurred, making it difficult to determine when the threshold has been crossed.

For example, the Soviets never attempted to plant nuclear weapons covertly on U.S. soil. Any effort to do so would have been viewed as an act of war. Indeed, Moscow's attempt to place nuclear weapons in close proximity to the United States triggered the Cuban Missile Crisis. Today, however, states are reportedly placing logic bombs capable of inflicting substantial damage into their competitors' computer networks for possible activation. Yet these actions are not viewed as an act of war.

Not only are states embedding cyber weapons on the soil of other countries, they are constantly using cyber tools to probe for network weaknesses and to extract data. The situation with respect to nuclear weapons is

very different. Since 1945 there has existed a de facto moratorium on the use of nuclear weapons, establishing a tradition of non-use. There is no tradition of non-use for cyber weapons; quite the opposite: cyber activity is ongoing, intense, and persistent.

There also exists, in the minds of many, a clear "firebreak" between the use of conventional munitions and nuclear munitions. No such firebreak exists in the cyber domain. Some aspects of cyber war are indistinguishable from the kinds of cyber attacks designed to inflict catastrophic destruction. For example, efforts to penetrate a computer system for the purpose of exfiltrating data are often indistinguishable from efforts to penetrate a system for the purpose of planting a logic bomb or executing a cyber attack (e.g., corrupting or deleting data, compromising a control system). This may make it difficult and perhaps impossible to discern promptly when a rival has transitioned from acts of cyber espionage, crime, and economic warfare to an attack on its adversary's critical infrastructure.

Compressed Engagement Timelines

One reason why both nuclear and cyber warfare favor the offense is that cyber attacks (like nuclear strikes involving ballistic missiles as delivery systems), occur along extremely compressed time lines. This further stresses the defense, which must be prepared to respond on very short notice.

When it comes to speed, cyber weapons trump nuclear weapons. During the Cold War nuclear-armed ballistic missiles could traverse the distance between the Soviet Union and the United States in less than 30 minutes. The two superpowers' forward-deployed nuclear ballistic missile submarines could strike their targets in even less time. Cyber weapons, however, can execute their attacks nearly instantaneously when the order to do so is given.

As noted earlier, while it is theoretically possible to smuggle nuclear weapons into a target area prior to an attack, the practical difficulties involved with such an effort, combined with the associated risks should the effort be detected, make it highly implausible. On the other hand, it is possible—and perhaps likely—that cyber weapons will be "pre-delivered"

into the systems they are designed to target. If this proves to be true, then it can be said that while a nuclear attack's command to attack precedes the deployment of the weapons, a cyber attack's process is likely to be reversed.

Given the speed at which cyber attacks can be executed, there is some discussion of building in automated courses of action (ACOAs) in cyber defenses somewhat like the human body's immune system, which responds automatically to threats to the body. These defenses would be authorized to take preventive measures, such as automatically rejecting requests that do not fit an approved profile, storing information on prospectively malicious actors who attempt to penetrate the network, and autonomously initiating defensive responses in real time.[233]

While automated responses may be the only way to defend against a cyber attack once the command to execute has been given, it is unclear how effective such responses might be. For example, the embedded cyber weapons may have instructions

233 Department of Homeland Security, "Enabling Distributed Security in Cyberspace," March 23, 2011, pp. 8-11, available at http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf, accessed on April 1, 2012.

to execute an attack at a predetermined time unless otherwise instructed. In such cases the attack order has already been given. Or an attack may be executed by an "insider"—a human with access to the computer system being targeted. The lack of information on the details of how cyber attacks might be conducted and whether automated defenses are likely to be effective quickly reduces the discussion to one of speculation. Despite this handicap, it does appear that when it comes to speed of attack, cyber weapons need not take a back seat to their nuclear counterparts.

The Arsenals and the Target Base

Nuclear and Cyber Weapons and the Target Base

As in the case of nuclear weapons, there appears to be something akin to a cyber arsenal, an inventory of cyber weapons that could produce catastrophic effects along relatively short timelines. Just as there are different kinds of nuclear weapons (e.g., fission and fusion weapons, those that emphasize radiation effects over blast and heat—i.e., "neutron bombs," weapons of vastly different yields, etc.), there appear

to be different kinds of cyber weapons as well, and for the same reason: to enhance the odds of creating the desired effect on the chosen target.

It seems likely that given cyber weapons' need to produce a wide range of effects there would be a wide range of cyber weapons as well, especially if the objective of those building the cyber arsenal is to have the ability to inflict catastrophic destruction on their enemies. Take one example, that of the SCADA systems that regulate many of the automated systems controlling key processes in various parts of the U.S. critical infrastructure. To the extent that there is a variety of these systems, each would require its own specially designed cyber weapon. For example, specific cyber weapons would be needed to target the financial system, where the likely objective would not be to physically destroy the target but to effect a "mission kill" by destroying confidence in the system (e.g., by corrupting or destroying financial data). These weapons would differ from those designed to corrupt a SCADA system regulating the controls of generators functioning as part of a power grid.

Nuclear weapons appear to be at a significant advantage in this comparison, as their requirements are far more general in nature (e.g., attack a point or area target, a hardened or unhardened target, maximize or minimize fallout, generate or limit casualties or physical destruction). Moreover, to the extent that the cyber target base engages in periodically upgrading to new SCADA systems, incorporating enhanced financial database security protocols, employing new computer operating systems, and the like, the greater the likelihood that the cyber arsenal will atrophy. Unlike nuclear weapons, whose declining effectiveness is more a function of the weapon's aging, cyber weapons do not age. The drawback with cyber weapons is that their target set is constantly changing in ways that risk rendering them ineffective or obsolete.

This suggests that cyber weapons' ability to cause prompt, catastrophic destruction may depend to a significant extent on a relatively stable target base, and/or on the ability to monitor closely changes in the base. This is not a trivial problem. It could greatly limit the ability of cyber weapons to produce catastrophic effects, or at least to do so along relatively short timelines.

By comparison, nuclear weapons' effectiveness seems relatively immune to changes in the target base. The focus of those assigned with determining how nuclear weapons should be employed is centered primarily on identifying targets, rather than identifying changes in the character of the targets.

In summary, those seeking to field a "strategic" cyber arsenal face a challenge that those overseeing nuclear arsenals do not: the need to constantly identify changes in the target base and develop new cyber weapons as necessary to threaten those targets.

Cost and Durability

While cyber weapons' effectiveness may atrophy far more rapidly than nuclear weapons, cyber weapons also are far less expensive to fabricate and maintain. This suggests that the number of competitors—both state and non-state—with access to cyber weapons is almost certain to be significantly greater than the number that possess nuclear weapons.

It also appears that while the competition between cyber offense and defense seems to favor the offense consistently, it also appears to be

highly dynamic—and perhaps unstable as well. For instance, if a competitor (especially a non-state entity) develops a particularly powerful cyber weapon whose effectiveness is likely to decline within a relatively short period of time, there could be a strong temptation to "use it or lose it" (i.e., use a particularly novel or effective cyber weapon before defenses are developed to counter it and/or the target base changes).

The value of cyber weapons may atrophy in another way that is not characteristic of nuclear weapons. Nuclear weapons of a particular design can be used effectively until the inventory of those weapons is exhausted; however, once a cyber weapon is used, similar cyber weapons may prove useless in future attacks if forensics efforts can identify how to neutralize them.[234] This may further contribute to a "use-or-lose" dynamic, thereby decreasing crisis stability.

234 On the other hand, there is some evidence that some cyber weapons may be more resilient. The Conficker worm has apparently frustrated all attempts by governments and "White Hats" (i.e., private cyber security experts) to break the command-and-control link between it and its originator(s). In so doing, Conficker's masters were able to maintain a robust cyber army that could be employed in executing several important missions (e.g., code breaking, DDoS attacks). Moreover, some worms apparently are capable (either autonomously or via command-and-control links) of modifying themselves over time, much as bacteria and viruses develop new strains to frustrate attempts to stamp them out once an initial version is identified. To the extent cyber weapons possess these characteristics, their effectiveness may depreciate at a slower rate than would otherwise be the case. Bowden, "The Enemy Within."

Weapon Effects

Assured Destruction, Collateral Damage, and Reversibility

The preceding discussion suggests that even with the current concerns over the reliability of the U.S. nuclear arsenal,[235] nuclear weapons are likely to be more reliable than cyber weapons. This distinction could prove critical in terms of a prospective attacker's willingness to undertake a cyber strike whose purpose is to cause catastrophic destruction.

Aside from being more reliable, nuclear weapons inflict damage that is likely to be far more severe and far less reversible than that of a cyber attack, even one that wreaks catastrophic damage. In addition to the use of a relatively small number of nuclear weapons to generate an electromagnetic pulse[236] covering a large area, a large-scale nuclear attack whose objective is to disable a large state's critical

235 In 2008, the secretaries of energy and defense declared "the United States does *not* have the ability to produce new nuclear weapons." Samuel W. Bodeman and Robert M. Gates, "National Security and Nuclear Weapons in the 21st Century," Departments of Energy and Defense, September 2008, p. 2. Note, however, that in 2007 the first W88 warheads with *replacement* plutonium pits and gas transfer systems were accepted into the stockpile. "Rebuilt W88 Formally Accepted for Use in U.S. Nuclear Stockpile," National Nuclear Security Administration, September 27, 2007.

236 "Electromagnetic pulses (EMP) are oversized outbursts of atmospheric energy . . . [Their] intense magnetic fields can induce ground currents strong enough to burn out power lines and electrical equipment across state lines." Dan Vergano, "One EMP Burst and the World Goes Dark," *USA Today*, October 27, 2010, available at http://www.usatoday.com/tech/science/2010-10-26-emp_N.htm, accessed on February 13, 2012.

infrastructure is likely to create far greater collateral damage (e.g., human casualties, residual radiation, physical destruction) than a cyber attack with the same objective.

In this regard cyber weapons may offer a sizeable advantage over nuclear weapons in that under some circumstances it may be possible for the side conducting the cyber attack to undo much of the damage caused by the attack, and to do so fairly promptly (e.g., restoring financial data, disarming a virus or worm). It also appears likely that it would be far easier for the victim of a cyber attack to restore its infrastructure than one who has suffered a nuclear attack.

Damage Assessment

It seems likely that undertaking damage assessment following a cyber attack directed against a state's critical infrastructure may not be especially difficult. For example, in cases where there is loss of power, loss of confidence in the financial system (e.g., large sums of money missing), ruptures in pipelines, a series of train wrecks or airliner crashes, etc., it

should be relatively easy to discern "battle damage." Similarly, assessing the effects of a nuclear attack would not be especially demanding, although this could change over time if ongoing work on nuclear weapons design in countries like Russia results in weapons with very low yields.

Second-Order Effects

The potential for a cyber attack to generate *unanticipated* second-order effects seems greater than that of a nuclear strike. While nuclear weapons also produce second-order effects, albeit in a different manner and on a far greater scale, these effects appear to be more predictable than those associated with cyber weapons.

In the case of cyber weapons, for example, efforts to limit corruption of U.S. financial system data could corrupt other countries' financial data; a cyber strike to knock out power in the U.S. would run the risk of turning out the lights in Canada and Mexico as well; compromising a state's air traffic control system could result in damage to, or even the loss of, the aircraft of foreign airlines operating in the targeted state's airspace.

Turning to nuclear weapons, a large-scale nuclear attack could generate enormous levels of dangerous radioactive fallout distributed thousands of miles from the attack site. In this example, the second-order effects themselves could produce catastrophic effects.

The second-order effects of a cyber attack could also result in catastrophic consequences. For example, if the inhabitants of the areas not affected lost confidence in the reliability of the infrastructure to the point that they felt compelled to develop an alternative structure for a particular function (e.g., finance, telecommunication) or to incorporate far greater levels of redundancy into the existing infrastructure. Here the "catastrophic" destruction would come in the form of a loss of confidence and the enormous costs associated with such a loss, and constitute "extreme misfortune" rather than "utter ruin."

Scale of Attack

The effects of a nuclear attack appear to be correlated to a significant degree with the number of weapons employed, their accuracy, and their yield. However, it is possible that even a single nuclear weapon could

produce widespread catastrophic destruction, for example through an electro-magnetic pulse (EMP) attack. Perhaps the prime example of this is a nuclear attack employing a single weapon detonated in the upper atmosphere. Properly executed, such an attack could generate a large electromagnetic pulse resulting in damage to electronic equipment over a wide area.

The effects of a cyber attack may be even less a function of the number of weapons employed than is the case with nuclear weapons, especially if EMP attacks are discounted. In part this is because a single cyber weapon—a worm—can be capable of multiplying itself and infecting a large number of systems. For example, the Slammer worm had a significant level of activity and compromised a large number of systems, while the Stuxnet worm may have started out as a single payload on a single thumb drive, but ended up attacking a significant number of targets within an air-gapped system.

Thus both nuclear and cyber weapons appear to share similar characteristics when it comes to how they might generate catastrophic effects. In both

cases the destruction caused by an attack would typically be associated with the scale of the attack. There are, however, notable exceptions in both nuclear strikes (i.e., EMP attack) and (especially) in cyber attacks.

Attribution and Catalytic War

As the discussion of attack attribution earlier in this report suggests, for at least the near term the source of a nuclear attack is far more likely to be identified than the source of a cyber attack. The difficulty in determining attribution of a cyber attack is a significant and perhaps enduring character of cyber warfare. This is due in part to the potential large number of actors that can execute cyber attacks, and to the relative ease by which cyber attackers can mask the origins of an attack. To date even substantial efforts to determine attribution of a sophisticated attack have not produced a "smoking gun" level of evidence, and have taken considerable time and resources to pursue.[237] This suggests that in the case of a cyber attack

237 Mike Lennon, "Massive Series of Cyber Attacks Targeting 70+ Global Organizations Uncovered," *Security Week*, August 3, 2011, available at http://www.securityweek.com/massive-series-cyber-attacks-targeting-70-global-organizations-uncovered, accessed on February 13, 2012.

whose purpose is to inflict catastrophic destruction, the victim may have difficulty determining its source. To the extent this is the case, the victim will also want to avoid being deceived into engaging in a catalytic war by retaliating against the apparent source of an attack that was actually conducted by a third party.

Moreover, cyber weapons could also be employed to trigger a catalytic nuclear war in other ways; for example, by feeding false information into a state's early warning system to spoof operators into believing their country is under attack when in fact it is not.[238] It seems unlikely that nuclear weapons could be employed to trigger a catalytic cyber war, at least given the current state of nuclear proliferation. This may change as more states or even groups acquire nuclear weapons.[239]

War Termination

During the Cold War concerns arose that if the United States and Soviet Union began employing

238 See, for example, David Eshel, "Cyber-Attack Deploys in Israeli Forces," *Aviation Week & Space Technology*, September 15, 2010.

239 That said, attack attribution may become a growing problem with respect to a nuclear attack as more and more countries acquire a nuclear capability. The problem of attack attribution in a proliferated world was the central trigger in the catalytic war described in Nevil Shute's popular novel, *On the Beach*. Nevil Shute, *On the Beach* (Portsmouth, NH: Heinemann, 1957).

nuclear weapons with the intent of using them in a "limited" way, they might not be able to stop. Attacks on an adversary's command and control system (to include its leadership), or breakdowns in communications (e.g., through an EMP attack) could, some believed, preclude the two sides from negotiating an end to hostilities, even if both sides desired it.[240]

Once underway, stopping a cyber war may prove just as difficult, although for different reasons. Assuming both sides were to agree to end hostilities, attacks would have to cease. This assumes, however, that both sides could control the hacktivists and patriot hackers acting on their behalf. This could be difficult, if not impossible, to achieve. Failing that, war termination might be possible if these groups and individuals could be identified by the two sides as independent of the belligerents *and* as not acting as surrogate belligerents. This would also seem difficult to accomplish. Moreover, given the difficulty in achieving attribution of an attack's source and the fact that, unlike nuclear weapons, cyber weapons

240 Fred Ikle notes this problem, as well as the challenge of communicating through intermediaries when direct communication is not possible. See Fred Charles Ikle, *Every War Must End* (New York: Columbia University Press, 1971), pp. 93-94.

and tools are employed routinely in "peacetime," it could be impossible to determine whether states have crossed the threshold between cyber war and cyber "peace" back into non-belligerency. Put another way, whereas the peace/war threshold is clear with nuclear weapons, it hardly exists in any meaningful sense in the case of cyber weapons.

There could also be a problem in "defusing" cyber weapons that had penetrated closed systems and, lacking a command link back to their masters, were programmed to activate at a particular time. Finally, were efforts made to recover or defuse such weapons it could be difficult for either side to convince its enemy that such efforts were not new attacks, as the similarities between cyber reconnaissance and data exfiltration and delivering cyber weapons are great.[241]

Summary

The preceding narrative finds that while there are some similarities between nuclear and cyber weapons, there are far more differences. For our purposes,

241 Committee on Deterring Cyberattacks, *Report from the Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010), p. 17; and Herb Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," Unpublished paper, n.d.

however, it appears reasonable to assume that cyber weapons can produce damage that meets our minimum definitions of "catastrophic" (i.e., "extreme misfortune") and "prompt" (i.e., over a period of weeks or perhaps a few months). Nuclear weapons, on the other hand, have no trouble meeting the most stringent definition of catastrophic, as they can inflict massive damage within hours, if not minutes, threatening the destruction of an entire society or state. Simply stated, it appears to be far more difficult for cyber weapons to achieve prompt, catastrophic destruction than nuclear weapons.

Despite the far greater capability and reliability of nuclear weapons, several differences between these two types of weapons suggests that a cyber attack whose objective is catastrophic destruction is *more likely* to occur than a nuclear attack whose purpose is the same.

First, the absence of a clear distinction between various forms of cyber attack combined with the large-scale and persistent use of cyber weapons has blurred the distinction between peace and war. It has done so to the point where legal counsel has been

sought to determine if cyber attacks are, in fact, an act of aggression.[242] While nuclear weapons have a strong tradition of non-use (i.e., there appears to have been a clear distinction for the major nuclear powers between conventional weapons and nuclear weapons) there are no such barriers in the cyber domain. Quite the opposite condition exists; one characterized by a tradition of constant and intense employment of cyber tools and weapons by a wide range of actors. Absent a clear line between "peacetime" cyber activities and wartime activities, the odds that a cyber skirmish could escalate into a full-scale cyber war would seem to be greater than that a conventional or irregular conflict would escalate to nuclear use.[243]

Second, the problem of obtaining prompt, accurate attribution in the event of a cyber attack may encourage risk-tolerant leaders to believe they can inflict major damage on an adversary at little or no cost to themselves. At the same time, the fear of triggering a

242 Jonathan A. Ophardt, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield," *Duke Law & Technology Review*, No. 3, February 23, 2010, available at http://www.law.duke.edu/journals/dltr/articles/2010dltr003.html, accessed on February 13, 2012.

243 Nuclear-armed states have, with few exceptions, avoided direct confrontation between their militaries, apparently fearing that even this level of contact would pose too great a risk of escalation to nuclear combat. The Cold War, for example, found the nuclear powers (the United States and Soviet Union in particular) engaged primarily in proxy wars or in military operations against the proxy forces of its rival (e.g., the United States against the North Korean proxy of the Soviet Union, the Soviet Union against the U.S. mujahedeen proxy in Afghanistan).

catalytic war will discourage risk-averse leaders from retaliating. This would likely further encourage risk-tolerant leaders, especially if they believed the leadership of the state they may target is risk-averse. This dynamic is far less likely to occur with respect to nuclear weapons as the attack source can be more readily identified based on information provided by early warning systems or nuclear forensics after the fact.

To the extent that there are far more actors armed with cyber weapons than there are with nuclear weapons (a situation that seems likely to endure given the cost disparity between nuclear weapons and cyber weapons), it will be easier to find a match between risk-tolerant attackers and their perceived risk-averse targets.

Third, owing to the perishability of weapons and the transient nature of the target base, a use-it-or-lose-it dynamic may exist and might encourage a cyber power to launch an attack before its advantage is lost. Again, the more risk-tolerant the attacker, the more likely it is that an attack will occur.

Unlike in the case of nuclear weapons, the cyber attacker can employ defenses that can mitigate, perhaps significantly, the effects of retaliation should it occur. These can range from shutting down power to certain computer networks to cutting off contact with the Internet until the danger has passed.

There is one difference between cyber and nuclear weapons that could reduce the odds of a major cyber attack relative to a nuclear attack. As noted above it may prove more difficult to stop a cyber war once it has started. This could act as a counterweight to those differences between nuclear and cyber warfare suggesting that cyber warfare is more likely to occur. On the other hand once a nuclear war is under way in which the attacker's purpose is to inflict catastrophic damage, stopping such a war may be irrelevant in light of the damage sustained by one or both of the warring parties.

CHAPTER 6 > **CONCLUSION**

The Internet has expanded exponentially over the past two decades in terms of both users and uses. Today, some two billions users rely upon the Internet for financial transactions, widespread automated regulation of key control systems, sharing and storing information, and communication, to name but a few of its uses. But as dependence on the Internet has grown, so too have concerns over the system's vulnerability. The cyber economy has proven a lucrative target for cyber criminals, and the storehouses of sensitive governmental and economic information have become lucrative targets for cyber espionage agents. As the military competition expands into the cyber domain, the question

of cyber warfare's destructive potential is clearly on the minds of senior U.S. policy-makers.

This report examines the question of whether we are on the cusp of a major shift in the character of warfare involving conflict in the cyber domain. In particular, it examines the growing concern among senior policy-makers and military leaders in the United States and in other major cyber powers that cyber warfare could rival nuclear warfare in its ability to inflict prompt, catastrophic levels of destruction upon states.

Despite these anxieties, the level of attention devoted to thinking about cyber warfare by the strategic studies community pales in comparison to that accorded to nuclear weapons in their first decades of existence. There are likely several reasons for this. The first is that, unlike the atomic weapons detonated on Hiroshima and Nagasaki, cyber weapons have yet to demonstrate their ability to wreak great damage on the world stage. Until the advent of a cyber "Hiroshima" or "Pearl Harbor," cyber weapons will likely continue to be viewed as more annoyances than heralds of Armageddon.

Second, cyber weapons fail to fit within traditional conceptions of weaponry. While the destructiveness of nuclear weapons can be seen and quantified, cyber weapons offer no familiar frame of reference.

Finally, and perhaps most importantly, the small strategic studies community of the 1940s and 1950s was better informed about nuclear weapons than it is today with respect to cyber weapons. Governments have been very reluctant to share information regarding their cyber weapons or activities. Nor can this information be gleaned easily elsewhere; cyber weapons require no large industrial base to produce, giving no indication of the number or type built, and can be tested in relative secrecy. Thus there is no easy way to determine their true power, especially since the critical infrastructure they may be targeting is constantly changing. This makes assessing their place in the military balance difficult, if not impossible.

Although it is difficult to undertake an assessment of a form of warfare about which relatively little is known, this report attempts to make some progress in thinking about the issue. Given the paucity of

information in open sources, any conclusions must necessarily be tentative in nature.

Based on the preceding analysis, and given the terms as defined in this assessment, there is reason to believe that the potential exists for a cyber attack to inflict relatively prompt, catastrophic levels of destruction on the United States and other developed world states with advanced infrastructures—*provided one accepts a broad definition of what constitutes "catastrophic" destruction*. Cyber weapons appear capable of inflicting "extreme misfortune" on a state by imposing very large, long-term costs. For example, by *repeatedly* disrupting critical infrastructure for short periods of time, cyber attacks could attrite public confidence in the reliability of said infrastructure. Recall the statement of General Alexander:

> What's technically possible? Take down the power grid, the stock exchange, and the Internet—*for a while*.[244]

244 Keith B. Alexander, "Cybersecurity Symposium Session 1," Keynote Address, Cybersecurity Symposium, University of Rhode Island, April 11, 2011, YouTube video clip, between 1:17:23 and 1:17:35, available at http://youtu.be/gcEFcDqlQC0, accessed on April 10, 2012. Emphasis added.

The costs of such attacks would be paid in terms of:

- *Accepting* the losses associated with repeated attacks;
- *Adapting* the infrastructure at substantial cost to reduce significantly the losses suffered in future attacks; or, in extremis,
- *Abandoning* relying on information networks to manage and support critical infrastructure (i.e., returning to the "1980s").

These costs are already being paid, albeit at a far lower level than would be the case in the event of a catastrophic attack. Most countries and firms are accepting the losses associated with cyber attacks as a cost of doing business. Some are working to adapt their systems to minimize their vulnerability at an acceptable cost. Few have abandoned their reliance on information networks.

In the context of the historical analogies discussed in this report, the state of cyber weapon development appears to most closely approximate that of air power during the 1930s. At that time the world

had experienced several decades of progress in aviation technology, and had seen air forces employed in World War I and in lesser conflicts (e.g., Ethiopia, the Spanish Civil War, Japan's invasion of China) following the war. Yet none of these conflicts saw a major power employ the full force of its air power against another advanced state as advocated by Douhet and Trenchard. Comparatively speaking, we are at the same point with respect to cyber warfare. The cyber domain has been an area of competition between states and non-state entities for some two decades; cyber weapons have been employed in minor conflicts and political and military leaders have made startling claims regarding the capabilities of these new weapons. But we have yet to see the cyber capabilities of a major cyber power employed in full force.

Concerns over a cyber "Pearl Harbor" are legitimate in the sense that just as the attack on U.S. military facilities on December 7, 1941, shocked the American public, a large-scale successful cyber attack on the United States would likely generate a similar sense of shock. However, just as the attack on Pearl Harbor did not inflict a decisive blow on the

United States, neither is a surprise massive cyber attack likely to do so.

Indeed, despite the assertions of some, it also seems likely that cyber weapons have nowhere near the ability to inflict catastrophic destruction as that of a major nuclear attack. A cyber attack against critical infrastructure is almost certain to be *much less* destructive than a large-scale nuclear attack. Moreover, the attacker's confidence in the cyber attack's ability to inflict catastrophic destruction is likely to be *far less* than that of an attacker employing large numbers of nuclear weapons. Simply put, nuclear weapons remain in a class all their own. When it comes to discussions regarding inflicting prompt catastrophic destruction, nuclear weapons are the gold standard, whereas cyber weapons barely qualify for a place in the conversation.

That said, we are *far more likely* to experience such cyber attacks than we are nuclear attacks. There are several reasons for this.

ATTRIBUTION. Since World War II states have refrained from employing nuclear weapons out of fear

that such weapons might be used against them. This is deterrence through the threat of retaliation. This form of deterrence requires that the victim, among other things, be able to identify the source of the attack. While determining the source of a nuclear attack remains relatively straightforward, attributing the source of a cyber attack is likely to remain, in the words of General Alexander, "costly and rare." Although even the remote prospect of being identified might be sufficient to deter a risk-averse leadership from committing a major cyber attack, what of highly risk-tolerant leaders—men like Adolf Hitler, Josef Stalin, Mao Zedong, and Saddam Hussein? The prospect of inflicting major harm on their enemies while escaping retribution could prove irresistible.

Risk-tolerant leaders may also be tempted to engage in catalytic warfare where they play the role of a third party covertly attempting to instigate or influence a war between two other parties. In a crisis between two powers, if one were to suffer a massive cyber attack, the natural inclination could be for the victim to assume the other state party to the crisis undertook the attack. This could provide another layer of insulation from attribution for risk-tolerant leaders.

PROLIFERATION. Related to, although distinct from, the problem of attribution is that of numbers. It is highly likely that many more states (and even non-state entities) will have imposing cyber arsenals than nuclear arsenals. With many more decision-makers possessing these weapons, it cannot but increase the odds they will be used.

The combination of large numbers of cyber powers (perhaps including non-state entities) and highly risk-tolerant leaders also suggests a significant potential for cyber proxy wars. While it is difficult to imagine a nuclear proxy war, this is not the case with regard to cyber weapons. In fact, it may be more the rule than the exception, as evidenced by Russia's probable use of proxies (e.g., the RBN) in the cyber attacks on Estonia, Georgia, and Kyrgyzstan. While cyber economic warfare has not been characterized by formal letters of marque,[245] it does appear that there is a willingness on the part of states to use proxies to better avoid attribution when stealing

245 Governments issue a Letter of Marque and Reprisal to a privateer, authorizing that person to arm and crew a ship for the purpose of attacking and/or seizing enemy vessels. Privateers had much in common with pirates, but there were two major distinctions. First, pirates operated without the sponsorship of any state; second, privateering was viewed as an honorable activity, whereas pirating was not. Privateering was at its greatest from the 1600s until the mid-1800s, when most European states renounced it.

state secrets, intellectual property, and other valuable information. Employing cyber proxies successfully could give risk-tolerant leaders an even greater incentive to engage in large-scale cyber war against an enemy's critical infrastructure.

Should a radical non-state entity acquire cyber weapons capable of inflicting catastrophic destruction, there may be little if any restraint on their use. Such groups may care little for avoiding attribution; in fact, they may actively seek "credit" for an attack. As these groups have no infrastructure against which to retaliate it is not likely that deterrence through the threat of punishment will prove effective.

ABSENCE OF A CLEAR CYBER "FIREBREAK." In the case of nuclear weapons, they are either being employed or they are not; there is a clear firebreak between use and non-use. This is not the case with respect to cyber weapons, which are in constant use. It may, therefore, be difficult for the leadership of one cyber power to determine when, in the mind of its enemy, it has crossed the line between cyber operations that are "acceptable" and those that will trigger

a major escalation in the intensity of cyber activity that could lead to catastrophic attacks. The picture is blurred even further owing to the fact that states are constantly under attack from many sources, not just one. The waters are made even murkier still by the similarities that exist between cyber reconnaissance operations and those designed to implant cyber weapons in a network, or to conduct an attack.

In summary, the concerns of many senior leaders with regard to the dangers of a cyber war appear to have merit. The damage wrought by a cyber attack against critical infrastructure, however, would almost certainly be *much less* than that of a large-scale nuclear attack. That said, it appears that a major cyber attack that would inflict catastrophic damage on the critical infrastructure of an advanced economy is both plausible, and much *more likely* to occur than a nuclear attack with the same objective. If this is the case, it is long past time for states to craft strategies to address this threat, and for the strategic studies community to devote far greater attention to this challenge to international peace and stability.

GLOSSARY

Advanced Persistent Threat (APT)—A group, such as a foreign government, with both the capability and intent to continually and effectively target a specific entity, often to conduct espionage or attack operations.

Botnet—A network of computers that have been forced to operate on the commands of an unauthorized remote user, usually without the knowledge of their owners or operators. A botnet usually has one or more controller computers from which the operator can give orders to, among other things, conduct cyber attacks by flooding a site or computer with messages (see DDoS). The computers on botnets are often referred to as "bots" or "zombies."

Closed System—A computer network isolated from the Internet.

Cloud Computing—The delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers as a metered service over a network (typically the Internet).

Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR)—The acronym used to describe the group of functions designated by command, control, communications, computers as well as intelligence, surveillance, and reconnaissance to coordinate military operations.

Computer Network Attack (CNA)—A type of computer network operation that seeks to disrupt, deny, degrade, or destroy information, computers, or computer networks.

Computer Network Defense (CND)—A type of computer network operation that seeks to protect, monitor, analyze, detect, and respond to network attacks, intrusions, disruptions, or other unauthorized actions that would compromise or cripple defense information systems or networks.

Cyber Space—Comprises all of the world's computer networks, both open and closed, to include the computers themselves, the transactional networks that send data regarding financial transactions,

and those networks comprising control systems that enable machines to interact with one another.

Cyber Warfare—The actions by nation-states and non-state actors to penetrate computers or networks for the purpose of inserting, corrupting, or falsifying data; disrupting or damaging a computer or network device; and inflicting damage or disruption to computer control systems.

Distributed Denial-of-Service (DDoS)—A type of cyber attack that employs a number of computers simultaneously to flood the victim (usually an Internet site, server, or router) with large amounts of traffic, thereby overwhelming the site's ability to respond and effectively shutting it down.

Electronic Warfare (EW)—Actions involving the use of the electromagnetic spectrum or directed energy to control the spectrum, attack an enemy, or impede enemy assaults via the spectrum.

Fifth Column—Members of a state who attempt to assist a foreign power in undermining their government from within. The term is a reference to the military use of a column four across when

marching. The fifth column represents an unseen column at work within the enemy's own ranks.

Human Intelligence (HUMINT)—A category of intelligence derived from information collected and provided by human sources.

Information Technology (IT)—The branch of engineering that deals with the use of computers and telecommunications to retrieve, store, and transmit information.

Information Warfare (IW)—The use and management of information technology in pursuit of a competitive advantage over an opponent.

Integrated Network Electronic Warfare (INEW)—A formal cyber war strategy adopted by the People's Liberation Army that consolidates the offensive mission for both computer network attack and electronic warfare under a single department of the PLA's General Staff (see computer network attack and electronic warfare).

Interconnections—Portions of a power grid that provide power to one or more nations. The

United States' power grid is composed of three interconnections—the Eastern Interconnection, the Western Interconnection, and the Electric Reliability Council of Texas Interconnection.

Internet Protocol (IP)—The primary network protocol used on the Internet. It supports unique addressing for computers on a network. Data on an Internet Protocol network is organized into "packets," each containing a header (providing information about the packet's source and destination) as well as other information and the message itself.

Intrusion Detection System (IDS)—A type of software that automates the intrusion detection process by detecting the patterns of attack of a particular attacker.

Intrusion Protection System (IPS)—A type of software that has all the capabilities of an automated intrusion detection process (see Intrusion Detection System) but can also stop potential attacks.

Logic bomb—A hidden file or software package that when triggered will set off a malicious function. Logic bombs are relatively small, and, as they do

not need to communicate with an external operator, are extremely difficult to locate prior to their detonation.

Malware—Malicious software that causes computers or networks to do things that their owners or users would not want done. Examples of malware include logic bombs, worms, and viruses.

Moore's Law—A long-term trend in computing hardware in which the number of transistors that can be placed on an integrated circuit doubles approximately every two years.

Payload—Code in malicious computer programs (see worm) designed to do more than simply spread the program. It may delete files on the host system, encrypt files, or send documents via email. A common payload installs a backdoor in the infected computer to allow the operator to control the host computer (see botnet).

Peer-To-Peer—A computer's ability to send information directly to another computer without that information first passing through a centralized server.

Phishing—An attempt to acquire information such as usernames, passwords, or financial records by disguising itself as a trustworthy website or email address.

Remote-Access Tool (RAT)—A piece of software that allows a remote operator to control a system and is installed often without a victim's knowledge.

Revolution in military affairs (RMA)—What occurs when the application of new technologies into a significant number of military systems combines with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict by producing a dramatic increase—often an order of magnitude or greater—in the combat potential and military effectiveness of armed forces.

Russian Business Network (RBN)—A cybercrime organization physically based in St. Petersburg, Russia and specializing in personal identity theft for resale.

Server—A computer usually accessed by a number of users in order to interact with the information stored on it, such as web pages or email. Servers

are usually meant to operate without constant human monitoring. Routers, which direct the movement of Internet traffic, are a type of server.

Signals Intelligence (SIGINT)—A category of intelligence derived from the interception of signals, whether between people, electronic signals not directly used in communication, or combinations of the two.

Single-Point Failure Systems—A part of a system whose failure can bring an entire process, facility, or network to a swift halt.

Smart Grid—A digitally-enabled electrical grid that gathers, distributes, and acts on information about the behavior of its participants in order to improve the efficiency, importance, reliability, economics, and sustainability of electricity services. The United States is currently looking into the possibility of developing a smart grid.

Spam—The use of email systems to send unsolicited bulk messages indiscriminately.

Spear Phishing—A targeted attempt to acquire information such as usernames, passwords, or financial record details by disguising itself as a trustworthy website or email address. Unlike phishing, spear phishing seeks to target or "spear" specific individuals by acquiring personal information prior to the attack and exploiting this knowledge to gain access to desirable information.

Supervisory Control And Data Acquisition (SCADA)—Software for networks of devices that control and regulate valves, pumps, generators, transformers, and robotic arms. SCADA software collects information about the condition of and activities on a system and sends instructions to devices, often to do physical movements. These instructions are sometimes sent over the Internet or broadcast via radio waves.

Traceroute—A computer network diagnostic tool for identifying the path and measuring the transit delays of packets across an Internet Protocol (IP) network (see Internet Protocol). Traceroutes can

be used to identify the source of cyber attacks and are often referred to as "traceback."

Virus—A self-replicating computer program that can spread from one computer to another by attaching itself to an existing program.

Worm—A self-replicating malicious computer program, which uses a network to send copies of itself to other computers often without the user's knowledge.

Zero-Day Exploit—A cyber security vulnerability that is exploited or used on the same day that the vulnerability becomes generally known. It can also be defined as a cyber attack that exploits a vulnerability (e.g., in Microsoft's Windows operating system) before that vulnerability is known by either the software writer or the target of the attack.

CSBA
Center for Strategic and Budgetary Assessments
1667 K Street, NW, Suite 900
Washington, DC 20006
Tel. 202-331-7990 • Fax 202-331-8019
www.csbaonline.org