Cyber-terrorism

Jack Jarmon

The Internet is a critical infrastructure necessary to the functioning of commerce government and personal communication and national security. The system is not secure. – Intelligence and National Security Alliance report, November 2009

In a 2002 report prepared by the Center for Strategic and International Studies (CSIS), Jim Lewis, a former official with the Department of State and the Department of Commerce wrote:

> The idea that hackers are going to bring the nation to its knees is too far-fetched a scenario to be taken seriously. Nations are more robust than the early analysts of cyberterrorism and cyber warfare gave them credit for. Infrastructure systems [are] more flexible and responsive in restoring service than the early analysts realized, in part because they have to deal with failure on a routine basis.[1]

Six years later, in its 2008 report, *Securing Cyberspace for the 44th Presidency*, the same CSIS concluded:

> Cybersecurity is among the most serious economic and national security challenges we face in the twenty-first century. Our investigations and interviews for this report made it clear we are in a long-term struggle with criminals, foreign intelligence agencies, militaries, and others with whom we are intimately and unavoidably connected through a global digital network; and this struggle does more real damage every day to the economic health and national security of the United States than any other threat. As one general put it in his briefing to us: *In cyberspace, the war has begun.*

Interestingly, the project director for the 2008 report was, again, Jim Lewis. The contrast of analysis is not only striking for its reversal of positions, but also in its tone. The 2008 report called for a profound reorganization of our national defenses that embraces a spirit of partnership between the US Government, its allies, and the private sector. It also urges a break with the past on issues of de-regulation, security classification, and the call for leadership in order to drive forward a comprehensive cybersecurity strategy. The authors also concede that the information age has forced us to re-think how federal government operates across boundaries within and outside itself.[2]

How such previous attitudes could have been overturned so radically in a relatively brief span of time reveals more about the dynamic of the information-communication technology (ICT) revolution rather than it does about errors in a particular expert's analysis. Not only the pace of technology but also the rate of growth and expansion of critical infrastructures, such as government, finance, energy, etc., have intensified our society's use and dependency upon ICT.

In cyberspace, the war has begun

What, then, is cyberspace? Metaphorically, it is the realm of computer transactions. Physically, it is the hardware, software, and transport elements that equate to the network architectures through which energy passes delivering information. However, less specific or technical - but as unerring, is the definition by the science-fiction novelist William Gibson who first introduced the term. In his 1984 book *Neuromancer*, he expresses cyberspace as a "consensual hallucination. …A graphic representation of data abstracted from the banks of every computer in the human system." Although both definitions can be considered true, for the purposes of this book the definition offered by the U.S. Joint Chiefs of Staff is the most appropriate for the following discussion:

> A domain characterized by the use of electronics and the electromagnetic spectrum* to store, modify, and exchange data via networked systems and associated physical infrastructure.[3]

This strategic definition, rather than Gibson's "hallucination," allows us to discuss cyberspace and attendant concepts with the same terms that we use to understand and express our notions about the oceans, the ecosystem, outer space, or other frontiers of human endeavor where serious challenges co-exist alongside opportunities for cooperation. However, to have a basic grasp of those concepts and terms, we need to devote some time and explanation to clarifying the elements and scientific principles that make comprehension of the current information/communication system possible. Also, such familiarity with the facts gives us a sense of the system's fragility and our own national vulnerability.

An understanding of cyberspace begins with an understanding of telecommunications. In cyberspace circuits, or routes, that information travels can be physical (copper wiring, optical cable) or radiation based (microwave, WiFi). Vulnerability to attack is a feature of the transmission medium. Physical connections are subject to tapping and severed connections. Radiation based connections can be disrupted from broadcasted electro-magnetic signals. Walter Morris, Computing

[1] "Cyberterrorism: How Real is the Threat," United States Institute of Peace, December 2004

[2] "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies Commission Report, Washington, December 2008, p. 78

* What is known as the electromagnetic spectrum is the combination of electric and magnetic fields. The reciprocal relationship between electricity and magnetism form the medium. When these forces are unified mathematically they create electromagnetic (EM) waves of radio and light. The oscillation of atomic interaction determines wave frequencies, which govern over such properties as visibility, energy, and can create the separate pathways, or wavelengths, along which information streams.

[3] Yannakogeorgos, Panayotis, *Technologies of Militarization and Security in Cyberspace*, doctoral dissertation, Rutgers University, April 2009, p. 28

Manager at Rutgers University, offers a wide-angle perspective on the domain of telecommunications:

> While cyberspace refers to a non-physical abstraction, it is achieved using computers networked via various means of communication. Information is exchanged between the nodes on a network in numerous ways, some physically connected and some using various radio transmitters/receivers.

Whether physically connected or radio transmitted, the integrity and security of these circuits are vested in the communication system's ability to redirect traffic to alternative pathways in the event of circuit failure. Whether a copper-based, wireless, or optical data transport environment, a network is resilient to outside physical attack and disruption due to this fundamental element - redundancy. A simple but significant feature, redundancy merely refers to the multiple paths by which information flows. As stated above, those multiple pathways can be copper wiring, radio frequency, or optical fiber. As long as communication flow has a reliable and alternate (redundant) route, the circulation of information continues as a matter of routine.

The material elements of these paths made little difference in the original scheme. The ability to withstand an intentional or natural onslaught and maintain operational stability by diverting a signal to an alternative routing system was the only concern in the early design, and is still the major concern today. What has changed is the growth of these networks, the volume of information transmitted, the threat vector, and our struggle to adapt to a new and perilous environment. These changes arose from the natural and irresistible forces of technological development and advancement.

Once optical cable made possible the transport of high volumes of data at the speed of light, the growth in optical fiber networks over copper cable systems surged robustly and irreversibly. The change over in technology set loose immense growth in the capacity and efficiency of I/C networks. It also unleashed a dependence on electronic networks, which is nothing less than a systemic addiction. Although optical fiber cannot yet replace copper in every instance, its impact on telecommunications has been momentous and incontrovertible. In a frequently used metaphor, wavelengths of light are the traffic lanes, which information travels along the information highway. When lanes become inaccessible or over-burdened with data, we use alternative routes by switching lanes or adding more. Adding more lanes, or in other words, widening the bandwidth was the solution and one of the drivers of investment craze of the late nineties. It, also, may have been a contributing factor to the over-investment and eventual implosion of the telecommunication industry.

What, exactly then, is it that streams along the information highway? In most transport forms, electronic messages are disaggregated into bits of data at the origin point - contained and sent in the form of small packets that have routing information in what is called a packet header. Routers along the network read the packet headers and relay the packets toward their destination. At the destination point the data is re-assembled as packets arrive to form the original message. A breakdown or interruption of transmission any place along the network will not cause a system failure. The data packets will simply be rerouted. Unless messages are encrypted or transmitted over virtual private networks (VPNs), information flows according to this mode of transport. The system's openness contributes to this resiliency as well as its vulnerability. VPNs are often considered more secure. However, as opposed to a packet routing system, if a message is intercepted at a point within a VPN or an encryption decoded before it reaches its destination, the message can be revealed and security is compromised.

The data packet system relies upon standardized communication protocols to assure operation and control. The Transmission Control Protocol/Internet Protocol (TCP/IP) is the common set of protocols (the rules governing the transmission of data between devices) invented in the early stages of development, and used today to form the global system of interconnected networks. It is the military grade protocol suite that transports packets of information between devices and throughout the network as it verifies correct delivery between servers. By reading the IP header, a routing device can determine the source and destination of each packet. The critical information in the IP header allows the transport layer of the TCP/IP, or "protocol stack" to operate across networks. The IP header is simply a string of numbers that machines, such as routers, read to direct packets toward their destinations and, hence, form connections. At the receiving end, the header carries information that also instructs the destination computer how to recreate the message from the incoming packet data.

These strings of numbers, by which machines communicate, are translated into letters by the Domain Name System (DNS) for easier understanding by humans. Therefore, rather than having to type 66.249.90.104 when accessing a search engine, you can enter the more user friendly Uniform Resource Locator (URL): 'google.com'. Thirteen root servers house the DNS databases, which facilitate translation between IPs and URLs. The former U.S. Department of Commerce agency, Internet Corporation for Assigned Names and Numbers (ICANN), allocates top-level designations such as com, org, edu, and so on, and maintains and updates the data. ICANN is now a private entity, and as a result of international pressure, has recently facilitated the movement from a less English-centric system of domain naming to accommodate other languages. The policy shift is a modest signal that there may be progress away from a U.S. - dominated Internet toward a spirit of international cooperation and a truly global public good.

The Inception of Cyberspace

In 1968 the Advanced Research Projects Agency (ARPA), which later became the Defense Advanced Research Projects Agency (DARPA), began work on what

would later become the modern day Internet. The project's goal was to invent a communications network, which could sustain physical attacks and survive malfunctions occurring at other points along the system. ARPAnet, as it was called, required a minimum level of security because the number of users were, initially small, trusted, and known to one another. Shortly after the inception of ARPAnet, the National Science Foundation (NSF) realized the potential impact this technology could have on university research. Unfortunately, to have access to ARPAnet an institution had to have a research contract with the Department of Defense. The disadvantage of having no contractual relationship with DoD put many universities outside the circle, or circuit, of research and information sharing. Under such conditions the full potential of these new skills and equipment would not be met.

In order to provide an apparatus to keep pace with the technology, the NSF created a successor system called NSFNET. NSFNET linked to ARPnet with a backbone network, which employed TCP/IP. From the start NSFNET was an instantaneous success and within a short time, became overloaded. The NSF realized it could not continue financing the build out indefinitely and, therefore, set plans for its commercialization.[4] By the 1990s companies called Internet Services Providers (ISPs) overtook an Internet, which previously had been dominated by government, university, and industrial researchers. These ISPs competed in regional areas based upon price and quality of service, and in the process signed up millions of customers. As Andrew Tannenbaum remarks in his seminal work, Computer Networks:

> Many people like to criticize the Federal Government for not being innovative, but in the area of networking, it was the DoD and the NSF that created the infrastructure that formed the basis of the Internet and then handed it over to industry to operate.[5]

As the modern Internet grew beyond its original, conceptual boundaries, features such as the capability to have voice communication or Voice over Internet Protocol (VoIP) were added. This made it increasingly depended upon the Public Telecommunications Network (PTN). The expanding interdependency between PTN and the Internet further elevates the risk of infrastructure vulnerability.[6] Since PTN has become more software driven, our reliance on computer networks has intensified. Increased usage demanded a need for larger scale of operations and resulted in the creation of more access points.

At its inception as a U.S. military project the Internet's security concerns were minimal. It was an open system because it was closed to others outside its small circle of users with authorized access to specific government-owned and sponsored large mainframe computers. Due to the government's original intension to keep the function and system limited and proprietary, much of the security issues we face today are inherited traits of a previous generation of development.

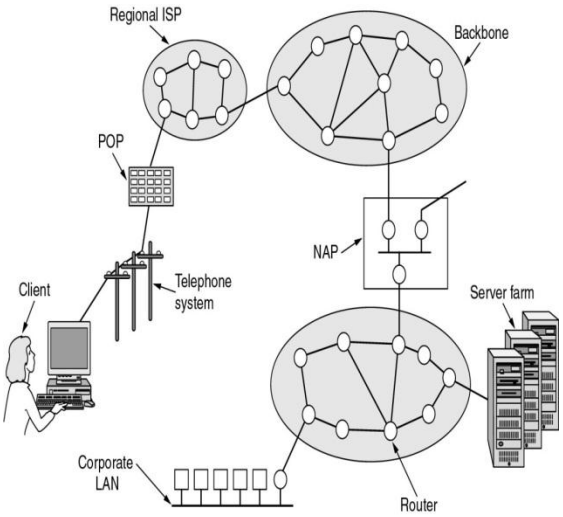
Today the Department of Defense, alone, has 15,000 computer networks and seven million computers and other network devices. DoD withstands more than three million log-ons each day.[7] For the above reasons TCP/IP, which lacks even base security controls, is perilously outdated.[8] It is from this design of over thirty-five years ago that the current network of connection support between autonomous systems and domain name services depends. Therefore, the Internet is inadequately secure by these current communication protocols. Despite our good intensions, in the haste to maximize its utility we have sacrificed resiliency and imperiled the stability of the many networks, upon which we so dearly depend. As if conceding these points, among its defensive strategy recommendations, the National Research Council goes as far as to urge: "Minimal exposure to the Internet, which is inherently insecure."[9] As a result of several top-level meetings (and, perhaps, in response to the NRC's recommendation) the Bush White House launched its National Cybersecurity Initiative (CNSI) during the waning days of its administration. The "cyber-initiative" included a dramatic re-scaling of the points at which federal networks connect with the Internet. The Office of Management and Budget set a limitation of 50 "points of presence" by June 2008. However, in March 2008, then Homeland Security Secretary, Michael Chertoff remarked: "we have no final number yet," with respect to a survey of all "points of presence."[10] According to Bruce McConnell, former chief of information technology and policy at the Office of Management and Budget, "Trying to catalog where things are so you can turn them off is a daunting task in and of itself."[11]

[4] Tannenbaum, Andrew, Computer Networks, Prentice Hall PTR, Upper Saddle River, NJ, fourth edition, 2003, p. 56-8
[5] Ibid, p. 56
[6] Nasheri, Hedieh, Economic Espionage And Industrial Spying, Cambridge University Press, 2005, p. 98

[7] Lynn, William, Deputy Secretary of Defense, in "US Creates Military Cyber Command to Defend Computer Networks," *Global Security*, 15 June 2009
[8] Hancock, Bill, "How to Stop Talking About-And Start Fixing cyber Security Problems," Cutter IT Journal (May 2006), in Yannakogeorgos, p. 212
[9] Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, National Research Council of the National Academies, The National Academies Press, Washington, D.C., 2002, p.150
[10] Harris, Shane, "China's Cyber Militia" in *National Journal Magazine*, May 31, 2008, http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php
[11] Ibid

INTERNET ARCHITECTURE

Source: Computer Networks, Prentice Hall, 2003



In the view of the above assessments, our present security challenges are unmet. No longer a closed research project, but rather a global public good, the architecture suffers from host of vulnerabilities. A report released on May 29th, 2009 by the Acting Senior Director for Cyberspace assessed the information and communication infrastructure as thus:

> Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations. Our digital infrastructure has already suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information. Other intrusions threaten to damage portions of our critical infrastructure. These and other risks have the potential to undermine the Nation's confidence in the information systems that underlie our economic and national security interests.[12]

In the absence of a major upgrade in system security the approach to security has been a "patchwork of niche products and work-arounds."[13] Such methods are responsible for many analysts claiming that security will always be a step behind attackers.[14] As Melissa Hathaway, lead member of the team, which prepared the 60-Day Cyberspace Policy Review for President Obama, stated:

> … our technical defenses have not kept pace with the threat, and it remains easier today – and I suspect for some time to come – for our adversaries to create an offense than for us to create a defense.

The April 2009 Cyberspace Policy Review Report and others have also called for a national comprehensive strategy that includes codes and best practices standards. Until these situations are addressed, the conclusions, doubts, and fears expressed above will remain.

Unfortunately, the barriers to amending the prevailing security environment are severely challenging to national governments and international commerce. The private sector primarily owns the electronic infrastructure, making security a business decision. In order to meet the demands of global commerce, corporate strategists are forced to favor their revenue generating units over investment in security. As long as the threat of catastrophe remains only an abstract fear, corporate boards will continue to view their responsibilities as vested in creating and accumulating assets, while leaving to subordinates the job of protecting those assets.

Equally unfortunate is that the public sector often takes its cues from the private sector. Deregulation of the telecommunications industry by obliging legislation and government agencies has over time helped to accelerate the growth of the Internet. Subsequently, the increased in the number of networks and access points only increases the opportunity and odds for an attack. This lack of regulatory oversight has had its impact on security. The lack of benchmarks to uphold security standards and the failure to create any incentives for industry to seriously self-regulate has consequences for national security. With only market incentive to drive the demand for improved and secure protocols, even existing methods and approaches to network security, although well known, are foregone.[15] New technologies that would create a more robust security network are, to the lament of many, under-developed. Rather than a distributed security dynamic, the current system is an assembly of off-the-shelf components in practice to maximize existing capacity.[16] Hence, partly because of over-dependence in market forces, the current system is left open and dangerously at risk. This benign neglect could, at some future point, be a root cause of a national catastrophe. Writing in 2006, Dan Verton remarked in *Black Ice: The Invisible Threat of Cyber Terrorism*:

> … the concept of allowing market forces to dictate security requirements remains the centerpiece of the [G.W. Bush] administration's policy on cybersecurity… government regulation of the Internet and software security requirements is out of the question.[17]

The author presses the point to suggest that such approaches to national security by the previous administration nearly abdicates any role it had for this

[12] Cyberspace Policy Review: Assuring and Trusted and Resilient Information and Communication Infrastructure, April 2009
[13] "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies Commission Report, Washington, December 2008, p. 58
[14] Nasheri, Hedieh, p. 51
[15] Making the Nation Safer, p.145
[16] Ibid, p.141, 152
[17] Verton, Dan, Black Ice: The Invisible threat to Cyber-Terrorism, McGraw-Hill, Emeryville, CA 2006, p.25

responsibility.[18] The continuing competitive pressure of the free market economy has forced the world systems of communication and transport to outgrow the apparatus of international laws, codes, and commercial best practices standards. These factors facilitated trade in the industrial age. However, in the information age, the clash of modern technology, economic imperative, and the current structure of interstate relations is a significant hindrance to reform. Despite the complexity of the threat and the problems that a vulnerable ICT infrastructure present, a security regime at any level will not have consensus support if, at the same time, it does not enable business. The policy dilemma is how to assure that information is secure and commerce is not compromised. Cyberspace today, as with the global supply chain, bears a set of formidable traits: enormity of size, opaqueness, complexity, and hence - vulnerability. It is another anarchic realm where states sometimes view cooperation as contrary to national interest. Global corporations can simultaneously be victims and unsuspecting abettors of crime. It is also an environment where the definition of what constitutes illegal activity, acts of war, and ownership of property rights and accountability remain obscure. Furthermore, in addition to these conditions is the complexity of a struggle with "intimate and unavoidable" adversaries noted in the CSIS's report. Adversaries in this case can be state and non-state actors, previous foes or traditional allies. The world has changed dramatically since the inception of the Internet with the advancements in technology. The upgrade in architecture, security, and policy should also reflect the change in culture and the new nature of competition.

The Militarization of Cyber Space

From its beginnings as a closed military project cyber space has undergone several generations of evolution. With the commercialization of the Internet in the early 1990s, the increase in efficiency, reduction of cost, ease of access, and inherent insecurity has shaped the way we must now approach our method of interaction and commerce and the attendant issues of national defense and global competition. Today, it seems ironic that as the Internet expands to become a vast public good that we may be faced with the prospect of its re-militarization. However, in this scenario the reality is far more threatening and the consequences far less fathomable. As national borders become blurred by the imperatives of global commerce and manipulated by the lure of transnational crime, so do the roles of state and non-state actors become complex and transformative. The transformation may well determine the way we assess power alignments, rules of governance, and the separation of human, sovereign, and individual rights of privacy.

Despite the hope that many had that the information age would bring with it new accesses to empowerment and a spirit of democracy, the trend is that these hopes may give way to a revived and ominous era of competition between states. Signaling these developments, in November 2008, the U.S.-China Economic and Security Review Commission made the following recommendation to Congress:

> The Commission recommends that Congress urge the Administration to engage in consultations with its allies on an alliance based approach to dealing with cyber attacks originating in China.[19]

The study further asserts that Chinese military planners believe the United States is waging a cyber-based war on their nation, and therefore, in order to protect their intelligence and infrastructure assets China must develop its own capabilities. These "capabilities" will not only allow China to defend its own exploitable weakness, but also wreck havoc upon the U.S. system, which they believe is extremely vulnerable because of its dependency on information technology. Additionally, the authors maintain that part of China's strategy is the contention that pre-emption is key to the success in an outbreak of hostilities, either, conventionally or with respect to cyber operations.[20] However, in a report compiled by Chatham House, the assessment is that China's primary focus has been in preparation for counter strike capabilities, rather than a first strike maneuver. Yet, the same report goes on to say:

> In order to offset its conventional weakness the PRC is transforming its armed forces from a mechanized to an "information" force and have stated they intend to use information "as a tool of war or as a way to achieve victory without war."[21]

In the post-Cold War era of conflict cyber capabilities are asymmetric capabilities that allow a less armed opponent to engage a stronger military foe effectively and successfully. The ability to disrupt, delay, or obfuscate conventional operations affords those with limited military power a menacing defensive and offensive advantage. Without the release of a single missile, bomb, or lose of life, the United States could be completely paralyzed. Our dependence on inter-locking networks for commerce, financial services, communications, utility grids, government and military logistical needs, leaves the U.S. a nation at risk. Whether they are private sector networks, unclassified government archives, or classified and secure systems – all are vulnerable to varying degrees. What is more, as the general interviewed in the 2008 CSIS report asserts: *the war has begun.*

Beginning in 2003, investigators believe that cyber attacks originating in China have systematically and routinely been launched against government targets in the U.S. This massive cyber-espionage operation, codename "Titan Rain," is the archetype of post-modern warfare. The operation illustrates not only the paradigm shift of technology and strategy, but also the potential

[18] Yannakogeorgos, Panayotis, *Promises and Pitfalls of the National Strategy to Secure Cyberspace*, Division of Global Affairs, Rutgers University, 2009, p. 9-10

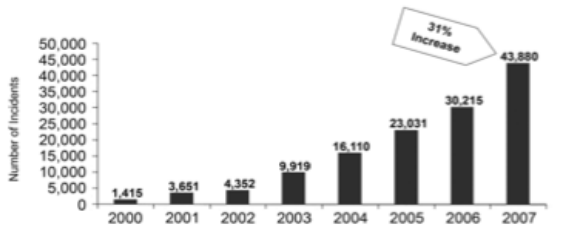
[19] 2008 Report to Congress of the U.S.-China Economic and Security Commission, p. 168

[20] Ibid. p. 166

[21] Cornish, Paul, Livingston, David, Clemente, Dave, Yorke, Claire, "On Cyber War," Chatham House Report, November 2010, p. 6

for power alignments and issues of governance for the extended future. More immediately, Operation Titan Rain reflects an inadequacy by our current defense structure to assess and respond effectively and even legally to such attacks. The assault calls into question issues over jurisdictional responsibilities, rights of privacy, and the roles of nation states and the private sector over accountability for security.

U.S. Department of Defense (DoD) Reported Incidents of Malicious Cyber Activity



Source: U.S.-China Economic and Security Review Commission, Hearing on China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities, *testimony of Colonel Gary McAlum, Washington, DC, May 20, 2008.*

According to a 2005 *Time* article, a mid-level systems analyst first uncovered Titan Rain while doing volunteer work for military intelligence.[22] Initially lauded by his government handlers for his work in discovering the intrusion, Sean Carpenter subsequently lost his security clearance and was fired from his job with Sandia Corporation. His offenses were the inappropriate use of company information and violating U.S. law by breaking into a foreign nation's computer system. Prior to his legal problems, Carpenter donated months of his time and energy to helping the Department of Defense and the FBI track down the source of these electronic intrusions. His investigation lead to the conclusion that information systems had been compromised from numerous U.S. Government agencies, including the United States Air Force, NASA, Redstone Arsenal military base, and also the World Bank. He believes the operations originated from Guangdong province in China and the information was warehoused somewhere in South Korea before finding its way back to Guangdong. Expert estimates claim that as much as 20 terabytes of information, or twice the print collection of the Library of Congress, was gathered.[23] Adding to his sense of betrayal by government authorities and company officials, Carpenter was dismayed that the investigative tools he acquired are not being used. After months of work he angers at the thought that no one: "…asked for the passwords or other tools that could enable them to pick up the investigative trail at the Guangdong router."[24]

According to the 2008 Commission Report to Congress, there may be as many as 250 hacker groups operating in China with either government support or "encouragement."[25] These individuals are often trained at Chinese military academies in cyber operations and the transference of such skills to the new arena of cyber war is seamless. As Robert Keohane and Joseph Nye have noted above, the environment of competition wrought by globalization has transformed and redefined military tactics. In their assessment it is not, necessarily, by design that "the asymmetry of global military power and the inter-connections among networks [has raised] new options for warfare." Yet, neither is it by mere random choice that they cite the Chinese in their examples as major players in the information war. The distrust from past conflict still lingers in the post-Cold War era of competition. Exacerbated by previous rivalries, today's thickening arena of increasingly, intensive and extensive web of international relations makes the combination of terrorism, drug trafficking, environmental degradation, and computer virus propagation attractive as well as cost effective and militarily potent.

In a conflict of such asymmetric weaponry the advantages of a cyber-strike are multiple and varied. Firstly, they can be launched instantaneously. A target would have little or no timeframe to prepare in defending itself. A second feature of an attack is the inability to establish attribution. Attribution, or the identification of the source of a cyber attack, is an issue of serious concern. Cyber attacks not only move at the speed of light, they occur in layers and travel along tortuously, indirect paths toward their objective. Since the current communication protocols lack the sophistication of the evolving array of hacking tools, it has become an increasing struggle for legitimate users to attribute incursions to a guilty source or point of origination. Therefore, by their nature, cyber attacks make it difficult for their victims to identify the enemy and, hence, retaliate appropriately. Finally, despite the absence of violence, cyber war can have the same destructive power as conventional warfare. Physical force, or a kinetic attack, aims to destroy an enemy's ability to wage war. Disabling a power grid, food supply, or any combination of elements of critical infrastructure can net the same result. Gen. James Cartwright, Vice Chairman of the Joint Chiefs of Staff claims that the consequences of a cyber attack could: "…be in the magnitude of a weapon of mass destruction."[26] Yet, these acts of aggression are without a multilateral consensus on whether they legally constitute acts of war.[27] The problem inhibits our ability to respond, re-organize our defense community, set standards, design and coordinate effective global cybersecurity policy, or fairly judge and discharge Sean Carpenter of his circumstances.

This asymmetric feature of cyber war is its most compelling for the United States. The strategic advantages once held by hegemonic powers in the interstate system are neutralized in the information age. The cost of "militarizing" cyberspace is low, and the

[22] Thornburgh, Nathan, *The Invasion of the Chinese Cyberspies*, "Time.Com," August 25, 2005

[23] Schifman, Jason, "The Need for a Strategic Approach to Cybersecurity," work in progress, University of Pennsylvania, April 2009, quoting Major General William Lord in "Air Force and the Cyberspace Mission Defending the Air Force's Computer Network in the Future," Center for Strategy and Technology, Dec 2007

[24] Thornburg

[25] 2008 Report to Congress of the U.S.-China Economic and Security Commission, p. 164

[26] Harris

[27] op. cit.

material resources are widely available. Therefore, the price of entry for less developed states and violent non-state actors is no longer an obstacle. Consequences of this paradigm shift in warfare are the proliferation of cyber warfare programs and development of non-traditional alliances between state and non-state actors, criminal gangs and terrorists organizations. [28] In this environment jurisdictional divides become meaningless to aggressors and create barriers for guardians of infrastructure assets and prosecutors of cyber crime. Furthermore, international codes of justice and best practices standards are unenforceable, and the attempts to establish order is uncoordinated and at times, insincere. As stated above, similar to the international supply chain, the system is plagued by its utter vastness and often, intended opaqueness. A colleague has described Cyberspace as: "an electromagnetic wilderness."[29] The authors of the CSIS report refers to it as:

> … part town square (where people engage in politics and speech), part Main Street (where people shop), part dark alleys (where crime occurs), part secret corridors (where spies engage in economic and military espionage), and part battlefield.[30]

Moreover, the technological threat vector posed by cyber war is metamorphic and tightly interlinked with the global economy. Adding to our dilemmas is the fact that the defense network in place to protect commerce and civil society is rooted in an interstate system encumbered by layers of formal protocol. Claims of national interest, state sovereignty rights, and political parochialism are the conditions of a former epoch and the mortmain, which hangs malignantly over the effort to adapt and meet the challenges of the new reality. Therefore, the conquest of this "wilderness" will require reorganizing society through policies that are more multilateral and, which can offer incentive for collaboration on a much grander scale. Otherwise, the alternative may be a partial return to Cold War power alignments and struggles with the addition of a cast of actors that include corrupt regimes, technologically sophisticated terrorists, and criminal organizations.

A Return to the Cold War

In the case of China, many analysts fear its leaders not only view cyber warfare as central to the overhaul of the national military, but also an important pathway toward economic development.[31] Aware of their comparative economic and military inferiority verses the U.S. the People's Republic of China (PRC) seeks to neutralize their disadvantages. By maximizing new realisms posited by the asymmetric environment of the information age, China hopes it can level the playing field.[32] A coeval of information technology has been the Revolution in Military Affairs (RMA). RMA is the application of IT to military purposes. The ever-expanding application of ICT and the rise of duel use technology have created a mesh of opportunities and risks ripe for exploitation. Since the end of the Cold War there has been a feverish effort by the American military to adapt its forces to the emerging paradigm. The effort has also been met by less powerful states and non-state actors, which recognize the relative competitive gains they can achieve militarily against traditional superior powers.[33] As expressed by the Chinese word for crisis, the confluence of these trends has offered up a convergence of opportunity and danger for China and its perceived rivals. It is a crisis that the PRC hopes to exploit against its adversaries on the one hand, and on the other hand, deflect as it seeks to defend its national interests.

According to Michael Pillsbury of the National Institute of Strategic Studies, China's own efforts to compete in RMA has resulted in projects known as *shashoujian* (assassin's mace). Having the project code number 998, *shashoujian* is believed to be a response to America's continued efforts in RMA and an important instrument in countering US hegemony in regional and global affairs.[34] Metaphorically, the term broadly refers to any action, technique, configuration of power, or technology deployed to overcome and reverse the tide of battle. The concept has been part of the discourse on military policy in China's since, at least, 2000.[35] In 1999 PRC President Jiang Zemin, a former Chairman of the Central Military Commission, declared:

> We should set great store by stepping up high technology innovation for national defense purposes and by developing technology useable for both military and civil purposes as well, and we should also master several *shashoujian* for safeguarding our national sovereignty and security as soon as possible.[36]

Compensating for its relative late arrival to cyber warfare, China attempts to gain parity with the US and Russia through projects such as *shashoujian*. For many in the military establishment, the inspiration for these efforts has origins in a Chinese proverb: "kill with a borrowed sword." The expression bespeaks of China's military policies that seek to overcome technological deficiencies with superior strategies.[37] "If you are limited in your strength, then borrow the strength of your enemy," so said Sun Zi, the legendary 2nd Century

[28] Yannakogeorgos, Panayotis, *Technologies of Militarization and Security in Cyberspace*, p. 14
[29] Ibid, p. 1
[30] "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies Commission Report, Washington, December 2008
[31] Schifman, p. 12-14
[32] Johnston, Alaster Iain, "Toward Contextualizing the Concept of a *Shashoujian* (Assassin's Mace), Harvard University Government Department, Aug. 2002, P. 27
[33] Kaldor, Mary, *Beyond Militarism, Arms Races, and Arms Control*, essay prepared for the Nobel Peace Prize Centennial Symposium, December 2001
[34] Ibid
[35] Pillsbury, Michael, *China's Military Strategy Toward the U.S.: A View from Open Sources*, US-China Economic and Security Review Commission, November 2001
[36] Johnston, p. 325
[37] Thomas, Timothy L., "China's Electronic Strategies," in *Military Review*, May-June 2001

BCE military strategist and traditionally recognized author of The Art of War. By taking the advice from an ancient text, China has girt itself to vigorously compete in the cyber conflict. As part of this strategy, the People's Liberation Army (PLA) has been establishing and cultivating relationships with patriotic hackers. "Hacktivism," or the combination of political activism and computer hacking, has evolved into a new phenomenon – state hacktivism. State hacktivism involves patriotic hackers who are motivated for nationalistic reasons, and operate in the service of their countries. In this practice area, China is particularly expert in organization and recruitment. The government sponsored Network Crack Program Hacker (NCPH), identifies proficient groups of hackers through competitions. Those selected receive monthly stipends from the PLA. According to Panayotis Yannakogeorgos of Rutgers University, they are recruited to not only ply their craft on foreign targets, but also to teach army cadets the tactics and tools for conducting cyber war. Joel Brenner, a former senior government counterintelligence official whose past posts include inspector general for the National Security Agency and chief executive of the Office of the Directorate of National Intelligence remarks about China's cyber-threat:

> Some [attacks], we have high confidence, are coming from government-sponsored sites. The Chinese operate both through government agencies, as we do, but they also operate through sponsoring other organizations that are engaging in this kind of international hacking, whether or not under specific direction. It's a kind of cyber-militia …It's coming in volumes that are just staggering."[38]

Not only as political rivals, but also as business partners, China has capitalized on the "borrowed sword" to breach security defenses and make gains in the struggle over cyber space. American and non-U.S. based ICT firms are often unwitting hosts of the strategy.[39] Competitive pressures force U.S. companies to rely on China's outsourced production facilities to assemble and manufacture products. Because of the efficiencies of the extended enterprise, the attractive pricing of products from developing countries and transition economies, and the dynamic of the global market place, Western companies are irresistibly lured into commercial alliances with non-Western partners. These joint venture arrangements are openings for a hostile player to implant viruses, malware, Trojan horses, and backdoors into equipment for proprietary civilian and military use. Once commercially available, the corrupted technology and component parts can infest systems anywhere in the world. The subversion of information systems is subtle, mostly impossible to detect, and potentially ruinous. The disabling of the U.S. Pacific Command Headquarters has been attributed to the use of malicious code produced in China.[40] According to some reports, a State Department official released a Trojan horse by opening an e-mail. This allowed a hacker covert access and denied PAC Command Internet use.

Through these same methods, Chinese hackers have also been credited with electronic intrusions against the State Department, the Department of Defense, Energy, Agriculture, Treasury, and Health and Human Services. For obvious reasons, the Pentagon and its sprawl of private contractors are particularly targeted. Boeing, Raytheon, General Dynamics, General Electric, and Lockheed Martin have all experienced attacks from cyber spies looking for sensitive information.*

Source codes, or the software programming instructions, are particularly appealing targets. The ability to copy or corrupt these millions of lines of instruction gives hackers the capability of tunneling into information systems around the world. Once the information is accessed, there is little to prevent someone from stealing intellectual property and inserting their own code. According to Google, this is precisely what has occurred not only to them, but at least 30 other California-based companies.[41] In addition, over the past several years, counterfeit Cisco routers have surfaced. Their intrusion creates the fear that implanted software could give foreign or other unauthorized agents the capability to tap into networks with the same ease as law enforcement agencies.[42] As required of network hardware manufacturers by law, Cisco Systems produces according to specifications that allow the U.S. government wire-tapping capability for investigative purposes. In such a case, a corrupted router: "could provide the perfect over-the-shoulder view of everything coming out of a network" according to Jeff Moss, a security expert with the Homeland Security Advisory Council.[43]

From a military standpoint, these capabilities can expose a nation to a new scope and dimension of threat. Quoting the commander of the Air Force Cyber Command: "You don't need an army, a navy, an Air Force to beat the U.S., you can be a peer force for the price of the PC on my desk."[44] What can, and perhaps has resulted is an "Internet too unwieldy to be tamed."[45] What may have also been unleashed is "espionage on a massive scale," says Paul Kurtz of the security consulting firm, Good Harbor Partners.[46] In support of these

[38] Harris
[39] Yannakogeorgos, *Technologies of Militarization and Security in Cyberspace*, p. 72-3
[40] Barret, Barrington M., "Information Warfare: China's response to U.S. Technological Advantages," *International Journal of Intelligence and CounterIntelligence*, 18 No 4, 2005
* These threats not only originate from China. The rise of new centers of design and production across the globe has created new opportunities for hardware and software manipulations by state and non-state actors.
[41] Markoff, John, Vance Ashlee, "Fearing Hackers Who Leave No Trace," *New York Times*, January 20, 2010
[42] Ibid
[43] Ibid
[44] Lord, William T., in "The New E-spionage Threat," *Businessweek*, April 2008
[45] Grow, Brian, Epstein, Keith, Tschang, Chi-Chu, "The New E-spionage Threat," *Businessweek*, April 2008
[46] Ibid

statements, current estimates claim Department of Defense computers undergo millions of scans on a daily basis along with thousands of potentially damaging probes.[47]

Although China is often cited as the greatest cyber menace to the U.S., Russia's military programs and adventures in cyberspace may have been the most conspicuous. The end of the Cold War, the restructuring of power alignments, and the passing of U.S.S.R. has not dismantled Russia's technological/industrial base or diminished its capability. The Russian assault on Estonia's e-government operations and electronic incursions into Georgia was early evidence of Russia's prowess and intent. It was also indication that the cyber world was becoming militarized and the fears of military experts were, perhaps, well founded.

During protests and retaliation for the removal of a statue at a Soviet era war memorial in Tallinn in 2007, not only were Estonian government ministry websites taken out, but those of political parties, news agencies, banks, and telecommunication companies also disabled.[48] Gen. William Lord is Chief of Warfighting Integration and Chief Information Officer for the Air Force. A minister of defense in this nation of 1.3 million reportedly admitted to him that "one million computers" attacked his country.[49] The electronic offensive by Russia raised alarms and cut at the core of the NATO alliance. Cries of concern about issues of collective self-defense rose to the surface and almost as quickly became muted because of a lack of definition, precedent, framework for resolution, and any clear policy guidance on an appropriate response. At the time there were also bitter disputes between Russia and former Soviet republics and Eastern satellite states. This electronic incursion may have been an act of frustration, or a signal to its rivals that Russia was prepared to open a new field of conflict to press its grievances. Prospects for how policy could be set to attend to future state sponsored incursions were faint, if not dark. As officials struggled to make public statements and offer assurances that the situation would be seriously addressed, the system of state relations was experiencing a new strain of "machtpolitik" that, in effect, stifled these policymakers and frustrated their efforts to act.

The year following the strike on Estonia, Russia combined military operations with a cyber attack against the Georgian government. Through a cyber-criminal organization known as the Russian Business Network, an electronic assault on government websites crippled Georgia's public information infrastructure.[50] Unlike the Estonian event, these attacks were coordinated with an armed invasion force. However, it was not the first time Russia employed cyber technology alongside military action. In 2002 a similarly orchestrated attack of armed kinetic force and an electronic incursion against servers occurred in Chechnya. As in the case of China, the Russian government has officially disavowed connection with any cyber offensive by itself or others working on its behalf.

Because of the U.S.'s lead in the information war, Russia's anxiety over the competition in cyber space arouses the same tensions, as had the Cold War period. The technology gap, national paranoia, recurring xenophobia, and a history of distrust have helped shape an emerging Russian worldview with roots in an old fortress state mindset. Foreign affairs correspondent, James Adams, writes:

> [Russian military officials] want to transmit a common message that Russia is a nation at war. It is an information war that the country is losing at home and abroad, and the current technology gap is comparable to the perceived missile gap of the 1950's that did so much to fuel the Cold War. This time, the race is not for space, but cyber space. And all the Russians are angry that America appears to be winning the war and that victory appears more assured every day.[51]

Therefore, Russia is considering building its own Internet in order to de-link from the present system. The Internet, which the United States designed, developed, and now controls 80% of the infrastructure, has become a security risk for Russia's national defense and strategic interests. Efforts at international conferences and summits to establish accords and norms for the regulation of cyber space have become tug-of-wars between the United States and Russia. Under dispute are not only the language of laws, but also the fundamental nature of their purpose. The U.S., naturally, opposes restrictions in a sphere of activity where it holds a compelling advantage. On the other hand, under-advantaged states push for a more regulated environment in order to lessen their vulnerability and exposure to cyber risks. In much the same way local industry might seek economic protection from its government against foreign competition with competitive advantages; Russia pushes hard in these negotiations for regulatory control. This tactic is usually regarded by the U.S. as an attempted "protectionist policy" that allows Russia to buy time while it works to narrow the technology gap and level the playing field.[52]

Some analysts believe, however, that this kind of shortsightedness by the United States may lead to an Information Age weapons race.[53] Other experts have already warned; "major governments are reaching the point of no return in heading off a cyber-war arms

[47] Lynn, William, Deputy Secretary of Defense, in "US Creates Military Cyber Command to Defend Computer Networks," *Global Security*, 15 June 2009

[48] "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian*, May 17, 2007

[49] Harris

[50] "Georgia's State Computers Hit by Cyber Attack," *The Wall Street Journal*, August 12, 2008

[51] Adams, James, "The New Arms Race," in the Next War: Computers are the Weapons and the Frontline is Everywhere," Hutchenson, 1998 in Yannakogeorgos *Technologies of Militarization and Security in Cyberspace*, 72-3

[52] Adams in Yannakogeorgos

[53] Thomas, Timothy, "Russian View of Information Based Warfare, *Airpower Journal*, 1996, in Yannakogeorgos, *Technologies of Militarization and Security in Cyberspace*, p. 72-73

race."[54] Such weapons in this conflict include the following:

- **Logic bombs**, which can be spawned by a Trojan horse. Once embedded within a system can damage circuitry or cripple operations at critical points and times. These are internal bits of code programmed to activate upon a certain condition, event, date, or time.
- **Botnets** are an array of computers, which run applications controlled by their owners that spy and disable networks and websites.
- **Trapdoors** bypass the security of programs under development. The developer's intension is to create a "hole" in the security framework of the program for exploitation at a future time. Only the creator of the trapdoor is aware of its existence once the program is in operation.
- **Bacteria** replicate itself and damages device storage resources by overloading disks and memory capacity.
- **Viruses**, unlike bacteria, carry malicious code. They can only attack programs or data in order to replicate themselves. Viruses pass through dormant and triggering phases before performing its function, in which results range from benign defacement to total system ruin.
- **Microwave** radiation devices burn out computer circuits from miles away.

In this intensifying high stakes game, there is also the belief that Russia is secretly enlisting China in support of its efforts to shape international policy on arms control treaties in cyberspace.[55] Whichever side prevails, the possibility to wreck havoc and plunge the world into a new epoch of confrontation is not only real, but already upon us.

However, December 2009 may signal a turning point in negotiations over the militarization of cyberspace. During this period, talks began between the U.S. and Russia regarding the possibility of international treaties to address the challenges posed by cyber warfare. Despite many contentious items, a common ground may be in the United States' interest to control Internet crime versus Russia's apprehension over cyber weapons development and proliferation.[56]

The parallels to the old order appear striking. Yet, at the same time, the configuration of power alliances would be a stark break with the past. According to a 2009 report commissioned by McAfee, Inc., criminal organizations are becoming more motivated by nationalistic pride rather than mere monetary gain. A prime example is Russia. The authors of the report cite McAfee's own Vice President of Threat Research, Dmitri Alperovitch who maintains that a righteous attitude toward the West is propelling much cyber crime. An indication of these moral postures is found in a warning posted on an online forum:

> We will recreate historical fairness. We will bring the USA down to a level of 1928-33.[57]

Spheres of influence would not be geopolitical but "virtual-political." Rather than bound by territorial jurisdictions and state borders, hegemons and their satellites would be linked by electronic connections. Whether associated by cultural and traditional ties, or motivated by unadorned, economic self-interest, the new order would be a constellation of states, corporations, terrorists, criminals, and social activists. Within this arrangement, it would be difficult for any single participant to have a monopoly on violence or arms control. Determining the extent and impact of the anarchy is impossible to suppose.

Net War and Net Warriors

Cyber space infrastructure is the critical underpinning of the global economy and, therefore, its integrity is essential to national security, public safety, and modern civic intercourse. The hyper-interconnection, which evolved parallel with globalization expanded opportunities for all. Whether those opportunities are used as a way for people to improve their lot, or destroy the quality of life of others is beyond its original design and control.

The asymmetry of today's warfare and the accessibility, anonymity, and ubiquity of the Internet has created opportunities for transnational crime organizations and international terrorism to plunder and recruit. Like state sponsored programs, these non-state actors have the capability to disrupt utility grids, telecommunications networks, defraud businesses and financial institutions, and disable and compromise government sites. Examples include:

- In 1995 the successful intrusion into U.S. Government files and downloading of sensitive information concerning North Korea's ballistic weapons research. The culprit was a sixteen-year-old British student[58]
- 1999 – the "Melissa" computer virus, which caused over $80 million in damages to personal computers, business and government networks by infecting e-mail gateways and clogging systems[59]
- An attempt to divert $400 million of EU funds from regional development projects in 2000. The funds were to be laundered through various online components of major money center banks, including the Vatican bank. Interdiction

[54] Ibid
[55] Markoff, John, Kramer, Andrew E., "U.S. and Russia Differ on Treaty for Cyberspace," *New York Times*, June 28, 2009
[56] Markoff, John and Kramer, Andrew, "In Shift, U.S. Talks to Russia on Internet Security," *New York Times*, December 132009
[57] "Virtual Criminality Report 2009,"Commissioned by McAfee, Inc., prepared by Paul Kurtz, Good Harbor Consulting, 2009, p. 12
[58] Schifman, p. 2
[59] Nasheri, p. 104

occurred only due to the misgivings of a co-conspirer who eventually, turned informant.[60]

- The financial support of the 2002 bombings in Bali, which police claim were provided by funds obtained through online credit card fraud[61]
- A Russian based hacking operation, which involved fraud and extortion in 2003. Aggregate losses amounted to approximately $25 million.[62]
- The 2004 investigation and termination of a criminal organization that involved 4,000 members engaged in stolen identities and credit card information. Known as "Operation Firewall," this Secret Service exercise culminated in the elimination of a major hub for online identity theft [63]
- The 2005 conviction of a Massachusetts juvenile responsible for the theft of personal information and initiating panic with bomb threats. The convicted hacked into Internet and telephone service providers over a 15-month period before being apprehended.[64]
- On May 2006, the Department of State believed its networks were hacked by unknown foreign intruders resulting in the download of terabytes of information.[65]
- May 2006, a public statement by a senior Air Force Officer reveals that "China has downloaded 10 to 20 terabytes of data from NIPRNet"[66]
- NASA blocks email prior to shuttle launches fearing harmful attachments in December 2006. At the same time Business Week reported that unknown foreign agents had obtained the plans for the latest space launch vehicles.[67]
- The Bureau of Industrial Security, which reviews high tech exports at the Department of Commerce, had its networks hacked by foreign intruders and forced off line for several months in April 2007.[68]
- In May 2007 "the National Defense University had to take its email systems offline because of hacks by unknown foreign intruders that let spyware into the system."[69]
- Reportedly, in August 2007 the British Security Service, the French Prime Minister's Office, and the Office of German Chancellor Merkel complained to the PRC about electronic intrusions.[70]
- A compromise of a major U.S. retailer's database that resulted in the loss of information of 45 million credit and debit card accounts in 2007[71]
- Databases of the Republican and Democratic presidential campaigns were hacked into by unknown foreign sources over the summer of 2008[72]
- In November 2008 classified networks at the DoD and CENTCOM were hacked and disabled for several days before the systems could be restored[73]
- The corruption of 130 ATM machines that produced fraudulent transactions in 40 cities in 2008[74]
- The estimated losses of $1 trillion due to intellectual property theft in 2008 [75]
- January 2009 – Israeli's internet infrastructure was paralyzed during that country's military offensive in the Gaza Strip. The attack, which concentrated on government websites, was launched from within the former Soviet Union and financially supported by Hamas or Hezbollah officials believe.[76]
- February 2009 –French combat aircraft were grounded following the infection of databases by a computer virus known as "conflicter."[77]
- March 2009 – Canadian researchers uncover a computer espionage system implanted in government networks of 103 nations. The researchers attribute the effort to China.[78]
- March 2009 – on a file sharing network in Iran, the plans for the new presidential helicopter, Marine 1, are discovered.[79]
- May 2009 – Unknown hackers gain access to the data in the Homeland Security Information Network (HSIN) collecting data on federal, state, and local employees and contractors.[80]
- June 2009 – the Applied Physics Laboratory of John Hopkins University had its networks penetrated and eventually forced to go offline.[81]
- June 2009 – Wolfgang Schaeuble, German Interior Minister, noted in a security report that

[60] Williams, Phil, "Organized Crime and Cybercrime, Synergies, Trends, and Responses," in Global Issues 2001, US Information Agency
[61] Cybercrime – Public and Private entities Face Challenges in Addressing Cyber Threats, GAO Report to Congressional Requesters, June 2007, GAO-07-705
[62] Ibid
[63] Ibid
[64] Ibid
[65] Lewis, James, "List of Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, http://csis.org/publication/23-cyber-events-2006, posted June 12, 2009
[66] Ibid
[67] Ibid
[68] Ibid
[69] Ibid
[70] Lewis, James, "List of Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, http://csis.org/publication/23-cyber-events-2006, posted June 12, 2009
[71] Cyberspace Policy Review: Assuring and Trusted and Resilient Information and Communication Infrastructure, April 2009
[72] Lewis, Op. Cit.
[73] Ibid
[74] Cyberspace Policy Review: Assuring and Trusted and Resilient Information and Communication Infrastructure, April 2009
[75] Cyberspace Policy Review
[76] Lewis, James, "List of Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, http://csis.org/publication/23-cyber-events-2006, posted June 12, 2009
[77] Ibid
[78] Ibid
[79] Ibid
[80] Ibid
[81] Ibid

China and Russia have been increasing espionage efforts and cyber attacks on German firms.[82]

- Critical infrastructure attacks on targets in the U.S. and overseas leading to outages at electrical power stations in multiple locations and cities[83]
- The FBI claim that Al Qaeda terrorist cells rely on stolen credit card information as financial support. [84]
- The CIA identification of, at least, two known terrorist organizations with the capability and intent to launch cyber attacks on the U.S. infrastructure [85]
- Due to cyber attacks, an estimated annual direct loss of $67.2 billion for U.S. organizations according to 2005 figures [86] and a revised figure of over $1 trillion worldwide for 2008[87]

Despite the volume of evidence to support justification for alarm, data on these assaults do not reflect the true scale of the problem. Public records are not only inaccurate due to detection issues, but often times by sheer intent. Reports are obviously lacking when victims are unaware of electronic intrusions. Frequently, because of manpower and technical skills deficit, cyber-crime goes on unmasked and with no ill consequences for the perpetrator. However, when cyber crimes do surface there are incentives for the injured party to keep these accounts out of the public realm. The consequences for victimized organization can be dismaying. The fear of negative publicity is always a concern for private sector enterprises as well as public offices and organizations. In the case of a security breach of a business firm, the instance can open an organization to lawsuit and adverse market impact. Studies at Georgia Tech reveal that firms that experience an interruption of operations will suffer an attendant decline in stock value. Furthermore, depending upon the duration of downtime, recovery can extend over several business quarters. This is particularly true if it involves a financial institution.

Public disclosure of security failure can also be a signal to attackers that vulnerabilities exist and an organization may be ripe for exploitation. With these circumstances also come fears of job loss and the demise of reputations. In weighing the costs and impact of reporting such incidents, it is easy to understand why many organizations opt to remain silent about their situation rather than draw public attention. Additionally, the allocation of time and resources, as well as the poor record of prosecution create further disincentive to report such offenses. The era of cybercrime has created a new set of legal problems and issues. Theft infers possession, which is a difficult, delicate, and more complicated argument when the property is intellectual rather than tangible. Furthermore, the information disclosed during the process of cross-examination can run the risk of be as damaging to the plaintiff's self-interest as the original crime.

Regardless of the reticence to admit to these victimizations, the economic loss to business and the consumer is still staggering. According to the GAO 2007 report, the direct losses due to computer crime, without an estimation of related costs, are $67 billion. Identity theft via electronic means amounts to over $56 billion. Worldwide, over $100 billion in losses from spam annually occurs. Spamming is more than a simple nuisance. Not only a malicious way to clog a system, span can act as a carrier for malware and a host of other cyber threats.[88] Dan Dunkel, President of New Era Associates, a security consulting firm says:

> With tremendous technical advantages come potentially devastating risks. As digital citizens we lack a fundamental "open" dialogue to confront the obvious trends in international cyber crime, or to address the complex technical, business and legal issues that will ultimately better secure cyberspace. We need to make cyber crime and security an international priority.[89]

As stated above, these numbers not only reflect an unknown percentage of unreported and under-reported incidents, they also represent a statistic, which continues to rise. The cybersecurity threat is outpacing our our attempts at a solution. It hovers over us at the national, organizational, and individual level. The global economy, and perhaps, our way of life may be at risk. A Senior Advisor at the Belfer Center at the John F. Kennedy School of Government at Harvard, Melissa Hathaway writes:

> I believe that we are at a strategic inflection point – and we must band together to understand the situation and ascertain the full extent of the vulnerabilities and interdependencies of this information and communications infrastructure that we depend upon. As I reflect upon the situation, one of the key recurring questions is whether we really understand the intersections of our critical assets and the networks and how we as entities interface with the communications infrastructure and the energy grid and other critical services that are provided on the backbone of interdependent networks.[90]

Understanding the power and opportunity of cyberspace infrastructure is not complete without an understanding its fragility and our vulnerability should it fail. The table

[82] Lewis, James, "List of Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, http://csis.org/publication/23-cyber-events-2006, posted June 12, 2009

[83] Cyberspace Policy Review

[84] GAO Report to Congressional Requesters, June 2007, GAO-07-705

[85] Ibid

[86] Ibid

[87] Hathaway, Melissa, *Five Myths About Cybersecurity,* Belfer Center for Science and International Affairs, John F. Kennedy School of Government, December, 21, 2009

[88] GAO Report to Congressional Requesters, June 2007, GAO-07-705

[89] Dunkel, Dan, President, New Era Associates, interview, December 2010

[90] Hathaway, Melissa, "Strategic Advantage: Why America should Care About Cybersecurity," Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, October, 2009, p. 1

below represents the various technique categories of cybercrime and a brief description of their methods and harmful effects.

Table
Techniques Used to Commit Cybercrimes

Type	Description
Spamming	Sending unsolicited commercial e-mail advertising for products, services, and Web sites. Spam can also be used as a delivery mechanism for malware and other cyber threats.
Phishing	A high-tech scam that frequently uses spam or pop-up messages[*] to deceive people into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. Internet scammers use e-mail bait to "phish" for passwords and financial data from the sea of Internet users.
Spoofing	Creating a fraudulent Web site to mimic an actual, well-known Web site run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source. Spoofing hides the origin of an e-mail message.
Pharming	A method used by phishers to deceive users into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed Web site when the user types in a legitimate Web address. For example, one pharming technique is to redirect users —without their knowledge—to a different Web site from the one they intended to access. Also, software vulnerabilities may be exploited or malware employed to redirect the user to a fraudulent Web site when the user types in a legitimate address.
Denial-of-service attack	An attack in which one user takes up so much of a shared resource that none of the resource is left for other users. Denial-of-service attacks compromise the availability of the resource.
Distributed denial-of-service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Viruses	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. A virus requires human involvement (usually unwitting) to propagate.

Vulnerabilities

Perhaps one of the primary roots of our vulnerability is SCADA, supervisory control and data acquisition system. SCADA systems are computer systems, which automate, monitor, moderate, and control industrial plant functions and critical infrastructure. The technology is ubiquitous. The power grid is particularly dependent upon SCADA. As with the original Internet, these systems were designed with little attention to security. Data is sent "in the clear," or over open pathways that rely on the Internet and often require no authentication.[91] Furthermore, for economic reasons and owing to an enduring spirit and environment of deregulation, SCADA systems increasingly depend upon commercial off-the-shelf (COTS) components as security patches and to optimize existing capacity.[92] [93]

The use of COTS as security countermeasures may not only be perilous, but also impractical according to at least one independent analysis. A study by the University of California, Berkeley and Carnegie Mellon University asserts that patching and frequent updates may be unfeasible for control systems in certain instances. Upgrades sometime take months of advance planning and require suspension of operations. Therefore, the justification for installing security patches may be negated by economic considerations or market demands. These patch updates may also violate manufacturer certification under certain conditions and open the operator up to litigation.[94] These concerns, combination of control systems' vital role in critical infrastructure operations, and the general awareness of the lack of security used in their design and support, make SCADA systems attractive targets for malicious hackers, criminals, or terrorist agents.

Additionally, SCADA not only manages the soft elements of the network, which are associated with disruption issues, but physical elements fall under these systems' controls as well. Therefore, physical damage may result in the destruction of infrastructure. The long-term consequences are networks, which have to be rebuilt, and their components must be remanufactured from scratch.[95] The fragility of the entire system is further compounded by the ironies of an open Internet. According to the National Research Council's Committee on Science and Technology for Countering Terrorism, these vulnerabilities are widely known and details on our

[91] National Research Council of the National Academies, Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, The Committee on Science and Technology for Countering Terrorism, The National Academies Press, Washington, DC 2002, p. 140-141
[92] Ibid
[93] Schifman

[94] Cardenas, Alvaro A. Amin Saurabh, Sinpoli, Bruno, Giani, Annarita, Perrig, Adrian, Sastry, Shankar, "Challenges for Securing Cyber Physical Systems," Report prepared by the Department of Electrical Engineering and computer Sciences, University of California, Berkeley, Department of Civil and Environmental engineering, University of California, Berkeley, and the Department of electrical and Computer Engineering, Carnegie Mellon University with a grant from the National Science Foundation
[95] National Research Council of the National Academies, p. 140

exposure are accessible to all on the World Wide Web. In the committee's 2002 report, it states:

> Product data and educational video tapes from engineering associations can be used to familiarize potential attacker with the basics of the grid and specific elements. Information obtained through semi-automated reconnaissance to probe and scan the networks of a variety of power suppliers could provide terrorists with detailed information about the internals of the SCADA network, down to the level of specific makes and models of equipment used and version releases of corresponding software. And more inside information could be obtained from sympathetic engineers and operators.[96]

Stephen Flynn, in his 2007 book, The Edge of Disaster, reveals in one example how precariously tethered national security is to the national power grid. He cites a 2006 report by Siobhan Gorman of the Baltimore *Sun*. In the report the NSA feared the installation of two supercomputers would overload an already extended power grid. Under such stressed conditions the agency concluded that the longest period of time the electrical infrastructure could forestall a collapse of the system was two years. In the event of a meltdown, it would take between 18 to 30 months to design and procure equipment, obtain permits and build a new power station. In the interim, the NSA's ability to process its work and operate normally would be severely hampered.[97]

The U.S. electrical power grid, according to Gilbert Bindewald of the Department of Energy's Office of Electricity Delivery and Energy Reliability: "was never holistically designed," and "developed incrementally in response to local load growth."[98] The result is a service environment of constant change and uncertainty. The system's complexity, decentralized flow control, and fluctuating dynamic of consumer usage contribute additional challenges to security. A sudden drop in voltage, either because of uncontrolled demand or the result of false information inserted into SCADA could cause collapse.

There are many examples where the manipulation of the computer code could have devastating effect on critical infrastructure. According to Bindewald: "electricity [is] the ultimate just-in-time production process".[99] The absence of flow control, and the lack of any large-scale storage capacity make the electric power grid unique and vulnerable. The same features that propel and permeate our commercial way of life are the symptoms of our deficient immunity to a cyber attack.

Today the power grid is decentralized, aging, susceptible to blackouts, reliant on SCADA, and under increasing demand due to the expanding digital economy.[100] Only by making the grid "smarter" or by changing the supply mix (using alternative energy sources) can the power infrastructure and our daily routines be made more secure. However, these are mostly longer-term solutions, and the vulnerabilities we face represent prevailing conditions.

Already, there have been several reports involving major power outages by Internet enabled intrusions.[1179101] Some relate to instances abroad. However, the August 15, 2003 power black outs, which occurred in the northeast U.S., have opened up a discussion about the grid's vulnerability to hacker activity. In the intelligence community, speculation persists that the outage can be attributed to China or agents working in collaboration with the PLA. The 2003 outage affected 50 million people in three states, including Canada. It covered a 9,300 square-mile area and had an estimated economic toll of between 6-10 billion dollars.[102] The cause of the power failure has, arguably, never been fully understood. However, many of those in the counterintelligence community believe the PLA gained access to one of the networks that controlled electric power systems. The result was the greatest blackout in North American history.[103]

Officially, no involvement by a foreign government or national has been cited. Rather, "overgrown trees," which came into contact with high voltage lines are credited with the failure of more than 100 power plants in Michigan, Ohio, New York, and north of the border. A widespread computer virus supposedly put the system over the edge by disrupting the communication lines used to manage the power grid.[104] Whether an ill-timed event or an event by design, the outage forced one industry analyst to assess "that security for the nation's electronic infrastructures remains intolerably weak" and to also emphasize that the incident confirms "government and company officials haven't sufficiently acknowledge these vulnerabilities."[105]

Another outage in 2008 also raised speculation of hacker intrusion originating from China. A power failure cut off 3 million customers of Florida Power & Light along the state's east coast. The company blamed "human error" for the disruption. However, there are some inside government and industry who maintain that hackers inside China, have devoted considerable resources to mapping and analyzing the U.S. critical infrastructure, and by mistake or with intension, may have set off the incident.

As discussed, the Chinese are not alone in their quest for advantage in cyberspace. In fact, it was also reported that computer intrusions penetrated European utilities in 2006, and that assaults similar to these might have a history as far back as the Cold War. According to a press report in 2004, a portion of the Siberian pipeline

[96] Ibid
[97] Flynn, Stephen, The Edge of Disaster, Random House, New York, 2006, p. 83.
[98] Bindewald, Gilbert, "Monitoring and Modeling of the Electric Power System," Presentation, October 28, 2009.
[99] Ibid
[100] Bindewald

[101] Hathaway, Melissa, "Strategic Advantage: Why America should Care About Cybersecurity," Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, October, 2009, p. 13. Yannakogeorgos, Panayotis, *Promises and Pitfalls of the National Strategy to Secure Cyberspace*, Division of Global Affairs, Rutgers University, 2009, p. 22-23.
[102] Flynn, The Edge of Disaster, p. 69
[103] Harris
[104] Ibid
[105] Ibid

exploded in 1982 with the use of a logic bomb.[106] Today, the field is populated with many competitors and combatants. The warfare is asymmetrical, unpredictable, and absent of any conventional wisdom – yet, the questions are always the same: Who is the enemy? What are their intent and objectives? How do we maintain our security while enabling our work and protecting way of life?

In summary, cyberspace has become the new battlefield because it is the core of critical infrastructure and industrial control systems. Although this has been the situation for decades, attacks have been randomly confirmed, and many more have gone unreported or undetected. Sources of attacks are myriad. Cybercriminals, disgruntled employees, terrorists, activists, organized crime, and state actors all have their own resources and motivations. Meeting the challenges of these security threats is achieved through prevention, detection, recovery, resilience, and eventually-deterrence. However, the war is asymmetrical and, at present, the technological advantage is with the attacker. Offensive action is easier, cheaper, and quicker than it is for defensive action.[107] This is partly due to the fact the range of possible targets is almost endless. It is also due to the obsolescence of the overall infrastructure and an early insouciant attitude toward security. A third frustration is the fact that the action/reaction cycle to the threat is so sudden that the very innovation used to address the original vulnerability can create further instability.

Conclusion

In cyberspace we are hyper-connected to a series of networks where lines between private and public security blur. At the same time the linkage in human affairs is organic, as competitive and complementary impulses drive events while we all undertake to ply at our work and live our lives. In common is our need to conduct business, power our households, access financial assets, provide and receive healthcare. Therefore, the security of these networks is central to our way of life. The fragility of these networks and our reliance upon them puts us in a perilous state. We are vulnerable to a host of threats from state and non-state actors, natural disasters, and our own overuse of valuable resources.

Moreover, the transition from the industrial age to the information age has been disorienting for strategists and policy makers. The imperatives of international trade and commerce have suppressed the calls for investment in security. Economic policies, which require unquestioned faith in the market and posited the belief in privatization programs, while heaping scorn on government and regulatory involvement may have put the system on to a precarious ledge. What exists is a cybersecurity understructure resembling a Rube Goldfarb contraption of patches and workarounds unsuited to accommodate the traffic demands of SCADA systems and custom large-scale implementations. As Mark Cohn, a thought leader and Vice President of Enterprise Security at Unisys Corporation remarks:

> The marketplace driven interconnectedness that we have been so excited about over the last twenty years combined with orders of magnitude changes in available bandwidth put some of those systems in to a mode their designers never envisioned: we can't unravel those trends and backtrack but we did, in fact, know how to build fault tolerant systems that in some cases never failed and could apply the same engineering approaches for a "smart grid" if it were possible to arrange the right political and economic circumstances.[108]

The landscape of town squares, Main Streets, dark alleys, secret corridors, and open battlefields that the CSIS Commission Report described, is not a static environment. It is dynamic, and instability is an accepted condition – for now. Many fear that without an open debate, the condition will remain chronic. As the above metaphor infers, cyber conflict ensnarls many actors, on varying levels, and in so many ways. Furthermore, because the environment is so target rich, the establishment of order may require new partnerships between the public and its government, a rewriting of legal codes, and new mechanisms for mobilizing society.

In addition, a frighteningly, deadly backdrop to the above scenario is the prospects that as sub-state actors are becoming key players, an inter-state cyber Cold War may have already begun. Under the conditions of asymmetrical warfare, nation states and cyber criminal groups can make for natural allies. Cyber war and cybercrime employ the same weapons and require the same skills. However, the skills and weapons may now be for sale. We may be at the onset of an inter-state war among past Cold War rivals and, simultaneously, engaged in an asymmetric conflict of non-state players. A cyber expert claims:

> Many of the challenges of cyber war mirror those of in cybercrime because nation states and cyber gangs are all playing from the same instruments. For instance, anyone can go to a criminal gang and rent a botnet. We've reached a point where you only need money to cause disruption, not know-how and that is something that needs to be addressed.[109]

The guerilla combat of the post-Cold War era is open to a much larger pool of participants, whose cover is the anonymity and ubiquity of the "net." The general awareness that the critical infrastructure is critically, vulnerable, is as tempting to prospective attackers as it should be unnerving to its defenders and users. The tension creates a gambit for all international players. For state actors it may become a grand game of "chicken" to see who would launch a first strike. Many experts claim in preparation for that moment, some nation-states have been surveying the landscape to identify vulnerabilities in infrastructure systems of

[106] Cardenas, Alvaro A.

[107] Cornish, Paul, Livingston, David, Clemente, Dave, Yorke, Claire, "On Cyber War," Chatham House Report, November 2010, p. 28.

[108] Cohn, Mark, Unisys Corporation, correspondence, January 20, 2010.

[109] "Virtual Criminality Report 2009," p. 11.

power grids and communication networks. In the words of an expert quoted in the McAfee report nation-states are: "laying the electronic battlefield and preparing to use it."[110]

All the while there has been a lack of public debate and an attendant void of national strategy. Further hindering the debate is even the lack of a functioning lexicon to express a crime, attack, or a justifiable retaliation in cyberspace. Rules of engagement, established responses, and notions concerning deterrence or collective security are presently moot points, which cannot be resolved until there is a framework for guiding doctrine and action. During this failed process classified information is kept secret, goes unshared, or falls between the cracks. The procedure for laying out a strategy is further stifled by bureaucratic divides and the walls erected among the military, law enforcement, national governments, and global commerce. As this "dialogue of the deaf" persists, the want for action languishes. While much of the discussions go on behind the closed doors of government, the public and the private sector continue to be the target of daily assaults, and will so for the foreseeable future.

Another factor limiting our response is a lack of verifiable and quantitative data. Because of the reasons cited above, governments, corporations, and other victims are hesitant to come forth and admit to their victimization. As a result much of the data on cyber crime is merely anecdotal. Anecdotal data can lead to alarmism and encourage military response as the only option. Such action might satisfy our fears and rage, but may not be appropriate and almost surely cause greater instability.

On the other hand, calls for consensus building are well worn throughout our history. Without the incentive of a mighty stick or irresistible carrot, agreements are seldom achieve and their importunity goes on ignored when demands are based on nothing more than irrepressible optimism. At present there are no such self-regulating mechanisms or pressures to force stakeholders into a consensus. The to and fro between a Doomsday reckoning and Utopian fantasy appears to represent the state and direction of the discourse. Without some analytical discipline to assess the threat cyber crime and cyberterrorism pose to us all, our best hope for positive steps might be somewhere in between.

As to the overall challenges of cybersecurity, for additional interpretation it might be wise to recall a fictitious dialogue between Socrates and a Greek aristocrat, Meno. Meno poses a question to the philosopher: "How will you look for something when you don't know what it is?" The stated and ensuing exchange is referred to as "Meno's paradox." In the current arena of conflict solutions are elusive. The competition over political and economic control by state and non-state actors, the expanding web of criminals, terrorists, disgruntled workers, hacktivists, *et al*, add to global security's version of that paradox. The combatants are indistinct. Their motives are often vague. Demands are rarely offered. The shadowy world of failed states and opaque cyberspace, has resulted in changing roles for states, altered the impact of NGOs on civil society, and created new spheres of authority, with which we have no history or experience.

As an example, crime and terrorism traditionally, abided by separate ontological norms and dwelled in two diverse and lawless realms. However, in today's security environment, these realms are beginning to overlap and the consequences are evolving into a previously, unknown blend of potent danger and plight for governments, the private sector, and civil society. What emerges has been called the crime-terrorist nexus and has been quietly expanding for years. As it unfolds, it creates a serious dilemma for security, law enforcement professionals, and their functional responsibilities. Obscured by a complex of motivational factors and a constantly morphing threat vector, this new menace poses a severe challenge to established protocols and approaches to national security.

Even though motives sometimes differ, the *modus operandi* of these sundry actors can be similar if not identical. The intensification of the globalization process and the emergence of cyber crime and warfare have enabled illegal activity - whether motivated by material gain or ideological incentive. Despite the overwhelming advantage of resources of nation states, law enforcement agencies, and legitimate global commerce and industry, technology equilibrates all players with a level battlefield of accessible and comparative weaponry. Furthermore, transnational crime syndicates and international terrorist organizations often reflect the same efficiencies as multinational corporations due to the similarities of disaggregate organizational structures, agile and de-centralized chains of command, and technologically trained "staffs." Moreover, the connection between the criminals and terrorists is more common and apparent as terrorists become more entrepreneurial and resort to self-financing.

The array of failed states, the role of multinational firms, the obsolescence of traditional militaries, the exploitation of jurisdictional divides and legalities, and the opaque circumstances that influence attribution of attack and response, are only some of the issues that create and impact this shifting global security paradigm. The result is an opening within the global system for criminals and terrorists to nest, proffer, and are poised to exploit. As law enforcement agencies and national security organs grapple with questions of jurisdiction and mission ownership, a new threat takes shape that does not comfortably conform to previous patterns of activity, analysis, and protocols for response.

Inhibiting the ability to interdict is the lack of experience with this kind of threat, and the paucity of data that could help create predictive modeling methods and tools. These new opponents are a multivariate network of plotters. In some cases, they may be unrelated, stateless, and widespread – and in other cases, not. As a result, Meno's question becomes a troublesome and persistent dilemma for the security and defense communities as a simple, hypothetical query evolves into a somber, global concern.

[110] Ibid, p. 3