Journal of Comparative Policy Analysis: Research and Practice
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/fcpa20

Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)

Chris C. Demchak [a]
[a] Center for Cyber Conflict Studies, US Naval War College, Newport, RI, USA

Version of record first published: 12 Jul 2012

To cite this article: Chris C. Demchak (2012): Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI), Journal of Comparative Policy Analysis: Research and Practice, 14:3, 254-269

To link to this article: http://dx.doi.org/10.1080/13876988.2012.687619

Journal of Comparative Policy Analysis,
Vol. 14, No. 3, 254–269, June 2012

Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)

CHRIS C. DEMCHAK
Center for Cyber Conflict Studies, US Naval War College, Newport, RI, USA

ABSTRACT *Cyberspace as a system has expanded exponentially across the globe as a massively complex universal substrate. It now demonstrates the surprises of large-scale socio-technical systems from electrical grids to just-in-time manufacturing supply chains, all of which increasingly support or are supported by cyberspace. These deeply linked, large-scale socio-technical systems (STSs) are creating nationally and globally interdependent "socio-cyber" systems (SCSs) by using cyberspace to improve efficiencies and lower costs. No longer can one assume a national infrastructure to be resilient when it is vulnerable to the four cumulating layers of surprises coming from a global socio-cyber infrastructure (GSCI). Critical research questions are posed for each of these layers of surprise as necessary for understanding conceptually and institutionally how to ensure resilience in any emergent GSCI that is fundamental to global security.*

A common myth about the internet core of cyberspace is that it was designed to survive a nuclear war. It was not, but the story is so widely accepted that the resilience of this increasingly critical national and international infrastructure has been until now regarded as settled. Today cyberspace has begun to show the surprises and high reliability challenges of a number of large-scale socio-technical systems (STSs) from electrical grids to just-in-time supply chains for manufacturing. As a technical substrate for most of civil society, cyberspace globally underpins critical systems for most societies and has become essential for societal functions shared directly across borders as well. The global financial system is one example, as are the global transport and energy systems. Having grown across the globe, cyberspace can now enable rapid dysfunction beyond borders and harm many nations at once.

Chris C. Demchak is co-director of the new Naval War College Center for Cyber Conflict Studies (C3S). She has published numerous articles on societal security difficulties with largescale information systems and a number of books, including *Designing Resilience* (co-ed. with Louise Comfort and Arjen Boin, 2010) and *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security Conflicts* (2011). Current projects include *Military Organizations, Complex Machines* in the Cornell Security Studies series. Demchak's research emphasizes comparative operational institutional learning, advanced use of tools and cognition, and system-wide resilience against normal or adversary imposed surprise.
Correspondence Address: Professor Chris C. Demchak, Strategic Research Department, Co-Director, Center for Cyber Conflict Studies, US Naval War College, Newport RI, 02841, USA.
Email: chris.demchak@usnwc.edu

ISSN 1387-6988 Print/1572-5448 Online/12/030254-16

http://dx.doi.org/10.1080/13876988.2012.687619

Cyberspace has matured into a global community of critical "socio-cyber systems" (SCSs) in urgent need of multiple layers of resilience. The conceptual and institutional responses of decision makers inside any SCS need to recognize the global and local nature of complex surprises and accommodate surprise in and across their organizations. Research needs to indicate how institutional decision makers can embed resilience throughout the global socio-cyber infrastructure (GSCI[1])) that is emerging across an increasingly digitized world.

Defining Resilience and Large-scale Socio-Technical Systems

Resilience for any system depends on the ability to mitigate an unusually disruptive event that may produce a harmful outcome. Creating a resilient socio-technical system requires that two capacities be ensured. The first is accurate, collective sense-making from fragmented information, and the second is rapid, effective, collaborative action. For both capacities, knowledge from multiple sources must be immediately collected, analyzed, and recombined to manage the surprising circumstances effectively (Comfort et al. 2010). Such knowledge development requires continuous established processes, consensual understanding and trust, and technological tools to be established and tested long before the system is challenged.

The increasing complexity of STSs challenges efforts to increase resilience. Complexity rises as the number, differentiation, and interdependence of its internal elements rise (LaPorte 1975). The more tightly these elements are tied to each other's activities or outputs, the more damaging any disruption could be to all of the connected elements of the system. All connections along a particular chain of exchanges could be delayed, diverted, or stopped if a disruption prevents the delivery of goods to each of the connecting nodes.

As the complexity of a human social, technical, or combined system rises, so do the difficulties for its members to know how to establish resilience to surprise. The routine capabilities of each participant of the ever more intricate system do not automatically provide foreknowledge about what could go wrong across all the critical nodes and their interdependencies. Without the required knowledge, collective sense-making is not accurate, nor can the speed of collaborative action be assured. If a surprise can cascade over enough nodes, it is a systemic event. The less a complex human-machine system learns from its interactions with other actors, the less well it can accommodate possible nasty surprises, and the less effectively are independent actions of other participants able to survive surprise.

Large-scale socio-technical systems (STSs)[2] particularly challenge efforts to ensure resilience. They emerge when formerly independent technologies and their associated human systems are combined to form an even more complex, larger, networked socio-technical system. The emergent combined group of interconnected systems acquires life-like attributes as a STS, often as an infrastructure for an industry or a community or region. They continue to grow, changing their environments directly or indirectly in an autopoietic process, and occasionally dying (Mayntz and Hughes 1988).

In a deeply cybered world, the challenge to gaining sufficient knowledge to accommodate nasty surprises rises dramatically. As disparate organizations

self-organize their human members, cultures, processes, assumptions, history, and technical systems together to form STSs, they are often unaware of the additional risks that any one of them is assuming. The seemingly narrowly focused socio-technical system becomes a much more important "*socio-cyber*" system, spreading beyond the original visions of the organizers. If sufficiently large, frequent, widely dispersed, and persistent, systemic surprises channel individual and group behaviors across enormous SCSs in directions not anticipated by the designers of the technologies used or the founders of the organizational structures.[3]

SCSs can be prone to single failures that cascade disruptively, disabling the system. The massively integrated AT&T phone system standardized the nation's phone networks over 50 years of sometimes hostile takeovers. Its internally tight coupling reached a brittle level when, in 1990, a switching failure shut down wide swaths of its Midwestern telecommunications (Kuhn 2002). The 1995 earthquake in the key port city of Kobe, Japan severely disrupted deliveries of manufacturing components critical to keeping Toyota plants operating far to the south. Toyota could not make cars, and, in turn, Toyota's dealers and suppliers could not function. Because Toyota is a central and controlling node in a "keiretsu" or corporate network, linking a large set of critical social infrastructure functions like insurance, subcontractors, and research, a long disruption would have severely damaged the entire Japanese economy (Tierney and Goltz 1997).

When national SCSs link critical processes across borders, a scaled up SCS emerges in a "global socio-cyber infrastructure", assuming risks commensurate with the scale and criticality of a globally integrated socio-technical structure. Critical links tighten, and, at a different scale, generate complexity and potential risk to the member nations' home SCSs. To this dynamic mix are added "*complexifiers*" in cross-border variations in culture, legal obligations, language, historical experience, local market operating processes, and institutions deeply embedded in local structures (Fountain 2001).

Distance complicates resilience because it hinders the ability to monitor the capacity of a partner to manage surprises that may be critical to maintain a chain of healthy interactions across a wide network. A GSCI is more likely to have disabling actions occur far from the source of negative effects. Human participants do not routinely see what is happening with their distant partners, and their computer systems can only report what they are programmed to monitor and transmit. Subtle indicators of impending risk do not travel well across borders. GSCI participants separated by time, distance, and mediating technologies are often less cognizant of indicators of emergent risk than if operating in their own local cultures.

In a GSCI, local operational decisions can work well for the immediate community, but disrupt the precision of operations across borders much further away in a process called "glocalization"[4] (Wellman 2002). For example, a local firm may find its operations are better off if technicians change security filters to restrict some data exchanges which, in turn, alters the timing of certain applications. While they are happily operating with new timing, the rest of the system is no longer receiving the information it expects. Other partners react to buffer themselves from their downstream partners, while they try to isolate the flaw (Demchak and Dombrowski 2011). The more global the system and the more gateways it includes, the harder it is for local nodes to see broadly how their actions can influence and be influenced by

others' choices in the design of critical connection paths across nodes (Dobson et al. 2007).

Cultural preferences also pose challenges for resilience across global systems. When key SCSs self-organize beyond their borders, shared cultural cues among fellow citizens vanish. The resulting risks from human choices can be particularly difficult to discern. For example, it took several major air accidents to realize the deference that nonwestern co-pilots automatically showed to senior pilots also meant that the junior pilot did not correct the senior, even when the flight was endangered. To counter such deeply engrained cultural axioms, the international airline industry established a new rule requiring the co-pilot to state their agreement with a pilot decision, and backed the rule with a sanction against landing in western nations, if not followed (Cushing 1994).

Distance challenges magnify resilience difficulties even more if the GSCI emerges largely as web-led and entangling, but mutually productive massive data exchanges. Not only is it hard to wander down the corridor to ask a question or fly a few hours to look at some processes, a large amount of potential indicators of surprise are deeply obscured in massive volumes of critical data exchanges occurring daily. When a GSCI forms among nations with deep connections into the connected nations' infrastructures, the societies themselves become vulnerable to surprises far beyond those likely to be noticed or previously experienced by the GSCI members. When Kahn's "tyranny of small decisions" occurs somewhere in this unmonitored GSCI, they can cascade to become "normal accidents" magnified on a global scale (Kahn 1966; Perrow 1984).

Cyberspace – Underlying Globally Critical Infrastructure

Cyberspace is the expansion engine of globalization, and deeply underpins economic growth as the meta-GSCI. When the web goes down, whole swaths of an economy cease to function. In early 2011 the Government of Egypt cut access to the internet (except the stock market) to control rising protests, and the Egyptian economy ground to a halt within hours. Money was not available because empty cash machines could not connect to the internet to order more bills with the necessary approvals. Hotels and airlines did not get their bookings or check ins. Hospitals could not check their internet pharmaceutical orders, and online banking within the country simply vanished. Consular offices could not provide emergency information to traveling citizens, and news reporting went dark for lack of outlets. Wireless phones were also shut off to stop the workaround efforts such as messages texted to foreign twitter sites or phone-based access to external internet sites. The dissolution of the GSCI inside Egypt for five days cost the nation nearly $100 million formally, despite having only about 3 per cent of its GDP dependent on telecommunications and internet services (Williams 2011). Not included in this estimate are losses in wages, suffering for day laborers with no savings, and a tarnished national reputation for political stability.

Cyberspace's reach and risks are unique for the infrastructures of both modern and modernizing nations. No system in human history that is so profoundly man-made, malleable, and deeply connected has spread so far. For American policymakers today, cyberspace is *the* GSCI underlying most other systems critical

to the nation. When a system is so central to economic and societal transactions, even natural accidents can ripple through otherwise unnoticed global connections to increase the diplomatic tensions between suspicious or hostile nations. For example, in 2008 the nation of Egypt was astounded to lose 70 per cent of its internet access when a ship's anchor cut undersea cables in the Mediterranean Sea, followed in days by four more cuts, this time in the Gulf of Oman. Over the course of 3–4 weeks as operators in the Middle East tried to reroute traffic, about 75 million people could not reliably use the internet for essential functions. After a multitude of conspiracy theories, that cable cut and four that followed in rapid succession proved to be a "normal accident" (Perrow 1984), affecting at least ten countries from Egypt to India. Maps are poor, and earthquakes or ship anchors cut cables routinely, requiring an undersea fiber optic cable to be shut down or "go dark" for weeks. The cable that would cause most damage if it were cut stretches 17,000 miles from London to Japan, and all the dependent nations are unaware that it serves as an internet lifeline (StaffEconomist 2008).

Resilience across the cyberspace GSCS is difficult because the electronic and social systems it must support operate simultaneously, each deeply intertwined with the others' growth and effectiveness. When a critical central element fails in a complex system, even minor technological fixes can exacerbate the problem. The loss of one of the five cables was due to operators trying to conduct maintenance, when their efforts had failed to route traffic around the other four broken cables at the same time (StaffEconomist 2008). These accidents are not unique, and could be understood systemically, but there is an overall lack of knowledge about surprise and vulnerabilities across cyberspace as a global socio-cyber system.[5]

Challenges for Resilience with Cyberspace as Global Substrate for GSCIs

Resilience in cyberspace faces major challenges that were built into the basics of the current global system due to the ideas about security of key early designers and the deep presumptions of the organizations they founded (Fountain 2001). Once basic designs are made concrete, the faster the technology is reproduced, scaled up, and widely distributed, and the less likely anyone will have the time or incentive to go back into the core and change these early design presumptions, even if they are basically insecure or encourage failures. Most of the resilience challenges bedeviling a SCS or GSCI today reflect the early visions of the baseline technology designers who never viewed the machines and software as something anyone would want or know how to attack. Cyberspace began as a pure document sharing mechanism for which security was about physical reliability, not human predatory behaviors.

In the development of the underlying technologies on which so many critical societal functions depend, sources of surprise were literally designed into the basic technical structures by the original designers of the three main operating systems – Microsoft, Apple, and Linux. These structures created a frontier-like shared knowledge space that precipitated shortcomings in trust, opaqueness in ownership, and impunity of malicious actors which bedevil the open web today. As such, the neglect of surprise in the creation of the baseline technologies also enabled four levels of surprise in complex systems that challenge progress toward solutions.

Trust Shortcomings Embedded in Baseline Technologies

Designed by friendly colleagues who largely knew each other, the internet grew on key nodes, processes, and content structures based on trust. With the academic focus on sharing, university communities designed and promoted the notions of software, computers, and networks as unalloyed positive, free goods. These early and later designers themselves would never take another person's wallet or contemplate hurting someone, and they did not anticipate in their designs that someone would try to do so using the internet.

The early designers viewed security physically. The perceived problems at the time inside the early internet were only sometimes erratic wired connections, accidents, or a need for locked doors on offices and stacks of computer logs periodically checked for computerized financial fraud. Early hackers were viewed positively as tinkerers who made the system better. Passwords written on paper were taped to screens or sent unencrypted across similarly unprotected email systems (Kemmerer and Vigna 2002). The social construction of the early internet world across both software and hardware creators and their eager business clients ignored the possibility that anyone would disrupt the underlying connections of technically confusing electronic systems. This rather utopian zeitgeist affected early computer designers who deeply embedded this free-from-fear character into their basic structures. They built systems with most internal elements openly sharing data in unmonitored ways inside basic gateway protocols, each dependent on critical central standardized processes. For the early Microsoft systems, the firm considered the major technical challenges to be solely memory, speed, and costs. The major external threat was simply the early market lead of the more secretive, monopolistic Apple system, whose security obsession was viewed as Apple's major weakness (Mills 2010). Over time, Microsoft's relative openness about the internal workings of its systems did indeed decimate the market for the more expensive and controlling Apple, thus confirming the validity of more openness. Microsoft's standardized operating systems spread widely, standardizing huge swaths of the global system by technology diffusion alone. Along with standardization was embedded the trust that no one would want to harm the system deliberately. Taken as proof that security could largely be ignored was Microsoft's prosperity (Schroeder 2000).

Apple, in contrast, had always been security conscious, but against the chance that business competitors would gain usable knowledge, not against malicious actors. Apple created its systems protectively, deliberately refusing to share its inner systems characteristics widely and always controlling entry access to the internal code of its systems. Inside the Apple technological core, however, trust is as present as it is more obviously in Microsoft because the designs presume that only Apple engineers would be inside the machines. Internally, applications share data freely as much as the early Microsoft files attempted to do. If the hard exterior is cracked by skilled bad actors, the interior applications are no more resilient than the competitors are (Barney 1999).

The third major technology, Linux, deeply embedded trust into its structures as the leading worldwide "open source" operating system which relied on volunteers for its security. Linux was created after the internet had expanded out of the hands of the universities, and after the 1990s' "cyber prophets" had widely promoted the

notion of a free internet for a new, glorious, global community (Rheingold 1993). Its original designer, Linus Torvald was one of many computer scientists persuaded by the naïve trust in the good intentions of most users in the web's community. Linux also reflected his Nordic culture's deep trust in the power of collective wisdom willingly provided. As a "FOSS" or a free and open source system, where anyone is able to open up and view all the basic code of any piece of software that is installed with any other, Linux has a secure design to the extent that volunteers in the form of proactive, civic-minded, and often self-taught computer science hackers test applications against errors for free (Bretthauer 2002). Since the code was and still is available to everyone based on the old UNIX systems of IBM, both good and bad actors could understand any holes in the system (Cross 2006). Resilience was assured to the extent that sufficient numbers of volunteers were timely and accurate in the patches they constructed against poor or malicious code.

For all three systems, trust triumphed over security. This observation is documented in the relative openness of Microsoft's operations, undermined by poorly secured baseline applications and global spread; in the Apple system's secrecy with its reliance on brittle external walls built before web browsers were allowed inside; or in the Linux system's complete openness undone by the inability of volunteers to match in volume and time the malicious behaviors or sheer complexity of a globalized web. Now Linux applications have tens of thousands of users accessing that open design, but unpaid security watchers are not always on the job, nor do they necessarily have the time to fix everything. The criminal or hostile programmers called "black hats" are often the chronically underemployed, under-occupied students, bored middle-aged computer industry loners, or even full-time crackers (hackers who steal credit cards) paid by the Russian mafia[6] or paying themselves with the returns from their exploits (Wales 2002). The Linux global open source community has no method of accurately vetting a claim to be a well-intentioned "white hat" hacker. Any "black hat" can be in reality "gray", i.e. posing electronically as a white hat hacker. Similarly, Microsoft's (MS) core designs neglected security from the outset and are still struggling to compensate globally. The increasingly global reach of a standard MS operating system, Windows, meant that it was so very easy to keep adding applications and network connections rapidly to cut processing time in half repeatedly. Returns on investment, however, also meant that little time was available to ensure that the rush to develop has not embedded more errors exploitable by bad actors. "Bugs" in the millions of lines of code often existed in even a single globally used program, making it relatively easy for a dedicated bad actor to find a way to exploit these programs in successful hacks (Lindner 2006). In order to avoid scrapping the system and starting over, MS systems designers inevitably now must act as if not every security hole will be found, and that it will cost more for the firm to close the unlikely hole than the discovery of the hole by black hats will cost the firm later (Model 2000).

The early internet backbone networks also added a layer of trust by relying on particular backbone computers, called Border Gateway Protocols (BGPs). Acting like commercial post offices often owned and run by large internet service providers (ISPs), these BGPs today receive messages from other computers listing the final destination desired for a piece of data and then negotiate the shortest route to that destination. Along the way, each BGP's tools and procedures "trust"

that the other BGPs are not lying, mistaken, or being manipulated by outside actors or insider administrators who change the responses (Goth 2003). This system's human administrators have enormous power in making sure that the automatic computer decisions are accurate and timely. They can, without oversight, tell their computer to pick different future paths around a particular BGP node for any number of reasons on their own recognizance. They can, in principle, program their node's reply to other BGPs to shun some nodes or even divert whole streams of internet traffic through hidden filters or log systems of other computers (Seltzer 2010).

That redirection can be accidental or, as has happened in recent years, it can be deliberate manipulation in violation of the trust buried in the BGP system. For a few minutes in 2004, a mistake by a Turkish ISP qua BGP hijacked most of the internet (Seltzer 2010). In April 2010, Chinese actors arranged for a number of BGPs to automatically route 15 per cent of the globe's internet through China Telecom's BGP nodes, allegedly enabling the mass copying of all the data as it passed through the Chinese server and back out into the rest of the world. Included in this stream were US military and National Security Agency (NSA) traffic along with a wide array of information valuable for future hacking (Halliday 2010).

A final aspect of a trust challenge of cyberspace comes from widespread ignorance about its true vulnerabilities as a GSCI. People suddenly and inexplicably (to them) deprived of critical services can easily grow hostile and accept the more malicious interpretations that emerge easily. Only five cables in total went down in the 2004 Turkish ISP incident, but the vast majority of harmed nations and users were those in the Middle East or India, not users at either end of these long-range cables in the UK or Japan. Especially powerful was speculation that Iran was the real target for disruption given that the US had cut the internet to Iraq just prior to its 2003 invasion (Oates 2008). One can only surmise what could happen if Iran had believed the US had deliberately slowed its internet and harm had occurred internally. Trust in the global underlying GSCI has national security implications.

Ownership Opaque to Outsiders

Across cyberspace, someone or some firm owns every set of cables, BGP nodes, servers, wires, software, applications, data, and even electrical systems fueling cyberspace. Each of these elements are not only owned, they are also maintained, altered, and disposed of by someone living somewhere under some national jurisdiction and legal regime. Far from the free world of an alternative universe, the practical reality of cyberspace is a hardscrabble world of competitors, designers, abusers, social controllers, trend watchers, and users. Each of them has a proprietary interest somewhere in keeping their share as valuable, as large, and as safe as possible for themselves. Cyberspace is not a shared commons (Goldsmith and Wu 2006). Even the backbone networks are not public interest nodes open to all everywhere. The BGPs take messages from other BGPs only if they have an arrangement with the other BGP, whether for pay, for mutual trade, or for reasons of national policy. If the BGP is owned by major ISPs with high volumes of traffic on their own, they can often negotiate fees or very lucrative trades in order to agree to transfer other ISPs' or BGPs' bits of data.

Widespread ignorance about this complex patchwork of ownership, legal regimes, and formal and informal rules of play throughout the cyberspace substrate profoundly hampers improving its resilience as a GSCI. Not only is there a lack of shared awareness regarding how an ISP may have a financial interest in how traffic is routed through their own node, rights of ownership mean in most of the democratic, westernized world that the owner does not have to specify how they have or have not prepared for accidents or attacks. Violating private property rights is a major difficulty in the westernized nations, even if the critical functions of the nation may be increasingly at risk. Within their own piece of cyberspace, even if their insecurities can cascade outward to harm others these owners are completely independent in their decisions (Nojeim 2010). Property rights trump wider societal rights as a norm especially in western democracies with major ISPs able to contribute to political campaigns. Barring a major disaster to use as leverage, western political leaders have shown a disinclination to force ISPs or others to increase resilience. Even the French government, known for its preference for centralized control, has been hesitant to dictate security responses to its private ISPs. It only requires the ISPs to have the technical ability to close down individual users or whole segments of their nets if they are asked to do so by the government.[7] Using emergency powers during the Arab spring of 2011, the Egyptian government shut off the nation's internet and cell phones by calling to ask the ISPs to go off the web as BGPs. In principle, any one of them could have refused. When property rights trump all wider social preferences, the resilience of the entire system rests on a hope that all these firms will spontaneously do individually what is collectively best.

Criminals protect themselves behind the same property rights as legitimate users; the appearance of legitimacy is conjured more easily by the complexity of cyberspace as the universal substrate GSCI. A common assessment of Russian ISPs is that they are fully compromised by the cybercrime mafia known as the ''Russian Business Network'' (RBN). While the RBN ISP serves its honest clients just like any clean ISP, it also allows known illegal networks to operate on the same fiber optic cables and enables massive cybercrime, botnets, and other attacks on the pockets, intellectual property secrets, private home computer data, and infrastructure controls of other nations. The arrangement stops a victim nation's security services from acting to disrupt the malicious behavior out of concern for the costly potential disruption imposed on all the legitimate clients of the corrupt ISPs.[8] Making the situation even worse is co-ownership across nations where many major ISPs or Telecoms own parts of ISPs or major telecommunications structures in other nations, or are the central distribution node for other ISPs. The complexity and power of ownership across the cyberspace substrate portion of any GSCI makes it difficult for governments to assess and then ensure where and how the overall system of national infrastructure and societal dependence is or needs to be made resilient.

Impunity[9]

Cyberspace offers bad actors, individually or collectively, relatively easy tools to use with impunity in acting maliciously against distant strangers (Eisenberg and Miller 1987; Gottfredson and Hirschi 1990). The globally open cyberspace substrate allows

attackers choices historically available only to superpowers or close hostile neighbors. They can with impunity freely choose the *scale*, *proximity*, and *precision* of their attacks. Attackers sit in foreign lands and choose to scale their attack organization from five to 5,000 other internet users, to operate at any proximity to their targets from five to 5,000 miles away, and to target with any level of precision from one firm, five individuals or whole cities, or all three with the same malicious weapons. They may take all the time they need in capitalizing on these advantages, sitting far from any likely defender security forces and using the internet itself to collect free intelligence data on the intended targets. Cybered bad actors create black markets in cyber weapons, amass and sell huge collections of infected computers as botnets, and generate and act on likely profitable or politically attractive target lists (Goth 2007).

Such impunity from punishment also comes from many kinds of operational cover offered by the complexity of the cyber GSCI. A wide range of methods to avoid identification and apprehension anywhere make it easy to hide technologically, socially, and politically, that is, in the huge volume of cyberspace "noise" and different encryption systems, in the naiveté of many users and insecure socio-cyber system nodes, and in among competing jurisdictions, political cultures, or gaps in law or policy concerning cyberspace. The role of a robust, global, cybercrime community in undermining resilience is more than just theft and taking over computers surreptitiously, a process called "pawning" (Broadhurst 2006). With little fear of police in cyberspace, now botnet gangs will fight each other rather openly; they technologically destroy competing malware in infected computers to preserve the pawned machines for themselves (Goodin 2010g).

Cybercrime is today the university for future cyber warriors, and the biggest technology testbed for future disruptive cyber weapons. In the latter half of 2010, the convergence of cybercrime delivery methods and a nation–nation conflict occurred. In the form of a worm much like thousands of others, a malicious software called Stuxnet travelled around the Middle East from infected thumb drive to infected computer and back until it finally found the control software of the newly installed centrifuges of the Iranian nuclear power plants under construction. While nothing blew up in this instance, the centrifuges seemed to wildly oscillate unpredictably for no apparent hardware or software reason, and had to be removed as untrustworthy, significantly delaying the Iranian nuclear program (Falliere et al. 2010). The worm proved that keeping critical systems offline is no guarantee of security without resilience. Stuxnet was designed to use the human-on-foot as part of the wider GSCI to breach the machine–internet air gap. With Stuxnet, the days of relatively benign cyber spying through software backdoors or through betrayals by trusted insiders, vandalism, or even theft has suddenly evolved into the demonstrated ability to deliver a potentially killing blow without being anywhere near the target.

Impunity means that a multitude of such malicious designers could be at work right now, capitalizing on the Stuxnet code which was leaked to the underground hacking community. As a model to be copied all over the world, the Stuxnet worm offers the possibility of distant enemies spending hundreds of staff hours and expertise to insert such applications all over one's nation and triggering their actions without notice[10] (Sanger 2010). Few have any idea of the possible consequences of such new weapons, if released and used routinely. The sheer lack of knowledge about

who is doing what is matched by widespread ignorance of the extent of the socio-technical systems that could be massively disrupted.

Resilience Needs to Accommodate Four Levels of Surprise in Cyberspace[11]

The combination across the cyberspace substrate of complexity with misplaced trust, opaque ownership, and socio-political impunity imposes four successive layers of potentially catastrophic surprises on nations that now depend on the global cybered system. These four layers begin with the "*basic*" surprises inherent in STSs as a first level threat. When these systems are coupled into national socio-cyber systems across *critical infrastructures*, they create the bottom two levels of surprise. The third level emphasizes the global problem with widely standardized, untrustworthy basic technologies and the human predilection to prey on others. Together they add to the first two levels with the massive onslaught of "*bad actor*" malicious actions creating a third level of surprise. On top of these three, and emerging in small, exquisitely skilled groups across the globally cybered world from the huge bad actor population, are the "*wicked actors*". These groups or individuals pose the most precise challenge to specific defensive responses. If they can reach through cyberspace to access an institution's defenses, they can get in, and once in they cannot normally be stopped unless they were disrupted before gaining access.

Resilience is the most economical and effective response to the first three levels of surprise. Only the fourth level of wicked actors needs disruption in addition to resilience in a cybered world. A GSCI cannot be secured against nasty surprises by disruption alone, but neither is security by obscurity an option if wicked actors specifically seek to disable a socio-cyber critical infrastructure or organization. In a deeply cybered open world, a democratic society needs to accommodate surprise across all four levels. Table 1 indicates the four levels of sources of surprise and the suggestions for surprise accommodation in literature and in emergent practice. It is copied in whole because the final section on future research will highlight some promising avenues for work suggested by this layering of surprise with research conclusions and observable trends.

Call for Research on GSCIs and on Institutionalization of Cyberspace Resilience

Policymakers across the westernized nations are slowly changing their perceptions of the scope and complexity of the national security challenge posed by cyberspace as a ubiquitous substrate under all societal functions (Brenner 2010). The success of Stuxnet has induced political leaders to confront a need to reduce their national vulnerabilities to catastrophic surprise in critical infrastructures and institutions from all four layers of possible sources. If such malicious software can take down whole energy systems at once, states have no choice but to respond (Porche 2010). The question is how.

Scholars across a wide range of fields including security and resilience research are needed to provide guidance and insights as these political leaders make policies. Implementing the cyber resilience actions outlined in Table 1 requires societal and institutional capacities at each level adapted to the surprises of that level. A number of areas urgently need research to develop these capacities. Below are four general

Table 1. Requirements for resilience and surprise management across SCSs' four layers of threat and complexity

Multisource threat categories in increasing uncertainty and surprise potential	**Cybered resilience action requirements (including disruption supplement)**
Complexity in large-scale socio-technical systems, LTSs (basic "normal accident" and cascading surprise-prone large cybered organizations)	1. Redundancy (of knowledge) 2. Slack (in time to respond) 3. Organizational discovery trial-and-error learning (DTEL)
(all above) plus *Criticality for nation in wide area socio-cyber infrastructure systems* CIP, critical infrastructure (protected status), High reliability industry, or operationally engaged military	(all above) plus 4. Collective sense-making 5. Rapid accurate mitigation, improvisation, and adaptation action 6. Frequent whole system practice for extreme events under urgent conditions
(all above) plus *high volume bad actors* operating from all over globally accessible cyberspace substrate (average to good skills, ubiquitous from script kiddies to vast majority of botnet masters, volunteer anarcho-hacktivists and less-skilled nation-states)	(all above) plus 7. Enforceable cyber hygiene 8. Underlying technology-secure design transformation 9. Comprehensive multi-organizational/layer learning for systemic generative innovation 10. Stratified two-way flow sensors/tagged-linked interoperable policy-guided gateways (e.g., democratically designed and supervised national cyber borders in international "cyber Westphalian system")
(all above) plus *Wicked actors* operating globally, persistently, and highly precisely (high threat persistent motivations, exquisite skills, ability to organize, access/evasion expertise, or wide deep harm propagation potential)	(all above) plus 11. Extensive wicked actor(s) OODA loop/business model/motivation knowledge collection and development 12. Selected controlled disruption under protective principle of international law 13. Collective understandings/undertakings with like-minded cyber responsible states

Source: Demchak (2012).

questions critical for future research, each tied to a layer of surprise across global socio-cyber infrastructures.

First, at the basic level of surprise, in what ways can human and machine sensor sets and local knowledge development processes and tools be structured so that redundancy of knowledge, slack time for innovative responses, and sufficient discovery trial-and-error learning (DTEL) will be in place when and where needed? Second, for critical infrastructure surprise, how can we develop and reliably disperse locally adaptable tools for immediate sense-making and action so that organizations under urgent conditions can collectively know what has happened and what could happen? As a corollary, what are the best institutional designs that empirically show

effective consultations on-scene between all critical actors? Where, when, and through whom can the ability to act rapidly and accurately be ensured, with real-time feedback for adaptive corrections in process?

Third, in order to diminish bad actor surprises by making harm difficult to achieve, what alternative transformational research paths are most likely to produce resilient, advanced, large-scale, manageable technological designs which adaptably, legally, and routinely regularize knowledge transfers into and out of socio-cyber systems to minimize surprises? What socio-technical lines of research are proving most likely to enhance the sensor sets and knowledge development essential for collective sense-making and accurate response action at national and cross-national levels?

Fourth, what is not yet known about how to develop and employ highly specialized disruption capacities against the "wicked actors" beyond national jurisdictions to ease the persistent threat pressure on the first three layers of sources of surprise? What tools, legal regimes, and institutional focus are needed to alter the motivations (legitimacy, need, confidence),[12] business model, and "Observation, Orientation, Decision, Action" (OODA) loops of wicked actor groups? How can demonstrably more resilient socio-cyber national systems share their best practices with other institutions or nations without also educating unknown wicked actors, given the range of socio-political–economic–environmental differences?

The need is urgent; resilience must be built into systems over time and in advance of critical surprises. The fear of cyber threats is creating the basis for eventual national sovereignty, but it is not clear whose principles of security, openness, and civil society will be embedded in the technologies of the coming cyber international system. What is clear is that Stuxnet's emergence, success, and rapid spread of the code among the black hat hackers has shown that malicious sources of surprise are gaining against the lackluster resilience of cyberspace today. We do not have much time to do the research and get our resilience in place.

Acknowledgment

Nothing stated here represents the policies or positions of the US Navy or any element of the United States Government.

Notes

1. Pronounced "jeh-skee".
2. The central attributes of a LTS (here called STS) are as follows. First, an identifiable social system with boundaries and internal coherence is made when heterogeneous small to mid-scale organizational activities (linked at their core by interdependencies among machine elements) consolidate into a highly interdependent and spatially wide-ranging network of essential relations. Second, the scale of these phenomena is such that they are extraordinarily complex and hence difficult to comprehend by average non-expert individuals, a situation affording the system considerable insulation from normal mechanisms of social control other than costly concerted efforts in times of crisis. Third, the system's inherent complexity and spatial reach increase the likely opportunity costs of predicting, mitigating, protecting against, or surviving the surprising outcomes of complex systems (Demchak 1991).
3. See Wohl (1981) for a discussion of how, in a complex system, the proportion of these unknowable outcomes will be high compared to a simpler system. See Heimann (1993) for a discussion of how component reliability contributes to the system's overall ability to avoid errors. See also LaPorte

(1975), Ting (2003) Felsenthal (1980), Harrison and Shirom (1998), Sagan (2004) and Dewett and Jones (2001) for discussions of redundancy and uncertainty implications in the structures and socio-technical processes of organizational systems.

4. I am grateful to Sandro Gaycken of the Free University of Berlin for adding this notion to this discussion.
5. Many emergent GSCIs are rarely recognized as huge systems, because their exchanges are largely conducted over the web and never monitored. One such community is the international large firm indemnification GSCI (reinsurers). Its members avoid costly local safety changes by insuring with a smaller set of large national insurance firms who reinsure themselves overseas with a smaller set of global commercial insurance firms
6. The enormous and ruthless Russian mafia is widely conducting cybercrime at sophisticated levels against the west.
7. Personal interviews with key officials at the French agency for cyberspace security, autumn 2010.
8. These criminal ISPs are labeled "bullet-proof hosts" by V. Kozok, a German information security expert (personal conversation).
9. Some portions of this discussion are based heavily on Demchak (2011).
10. For example, as the critical infrastructure of westernized nations such as the US is moving online for automated 24/7 services with less labor or greater precision, the loss of a central server for the infrastructure of even small communities could prove devastating. In early 2010, a thief stole the one single computer running the automated system providing clean water for the town of Molalla, Oregon, USA (KPTVstaff 2010).
11. This section is drawn largely from Demchak (2012), especially the table.
12. These three map across a number of social science literatures, from international relations (God, butter, guns; or constructivism, liberal institutionalism, realism) to gang warfare (referent group, life options, ego) to social relations (religion, wealth, empowerment) (see Demchak 2011).

References

Barney, J. B., 1999, Looking inside for competitive advantage, in: R. S. Schuler and S. E. Jackson (Eds) *Strategic Human Resource Management* (London: Blackwell Publishing), pp. 129–143.

Brenner, J. F., 2010, Why isn't cyberspace more secure? *Communications of the ACM* **53**(11), pp. 33–35.

Bretthauer, D., 2002, Open source software: A history. *Information Technology and Libraries*, **21**(1), pp. 3–11.

Broadhurst, R., 2006, Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management*, **29**(3), pp. 408–433.

Comfort, L., Boin, A. and Demchak, C. C. (Eds), 2010, *Designing Resilience for Extreme Events: Sociotechnical Approaches* (Pittsburgh, PA: University of Pittsburgh Press).

Cross, T., 2006, Academic freedom and the hacker ethic. *Communications of the ACM*, **49**(6), pp. 37–40.

Cushing, S., 1994, *Fatal Words: Communication Clashes and Aircraft Crashes* (Chicago, IL: University of Chicago Press).

Demchak, C. C., 1991, *Military Organizations, Complex Machines: Modernization in the US Armed Services* (Ithaca, NY: Cornell University Press).

Demchak, C. C., 2011, *Wars of Disruption and Resilience; Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press).

Demchak, C. C., 2012, Resilience, disruption, and a "cyber Westphalia": Options for national security in a cybered conflict world, in: N. Burns and J. Price (Eds) *Securing Cyberspace: A New Domain for National Security* (Washington, DC: The Aspen Institute).

Demchak, C. C. and Dombrowski, P. J., 2011, Rise of a cybered Westphalian age. *Strategic Studies Quarterly*, **5**(1), pp. 31–62.

Dewett, T. and Jones, G. R., 2001, The role of information technology in the organization: a review, model, and assessment. *Journal of Management*, **27**(3), p. 313–346.

Dobson, I., Carreras, B. A., Lynch, V. E. and Newman, D. E., 2007, Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, **17**: 026103.

Eisenberg, N. and Miller, P. A., 1987, The relation of empathy to prosocial and related behaviors. *Psychological Bulletin*, **101**(1), pp. 91–119.

Falliere, N., O Murchu, L. and Chien, E., 2010, *W32. Stuxnet Dossier: version 1.3*. online. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (Symantex Inc.).

Felsenthal, D. S., 1980, Applying the redundancy concept to administrative organizations. *Public Administration Review*, **40**(3), 247–252.

Fountain, J. E., 2001, *Building the Virtual State: Information Technology and Institutional Change* (Washington, DC: Brookings Institution Press).

Goldsmith, J. L. and Wu, T., 2006, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press).

Goodin, D., 2010, Upstart crimeware wages turf war on mighty Zeus bot: All your bots belong to us. *The Register* online, London. http://www.theregister.co.uk/2010/02/09/spyeye_bots_vs_zeus/

Goth, G., 2003, Fixing BGP might be difficult – or not so tough. *Internet Computing, IEEE*, **7**(3), pp. 7–9.

Goth, G., 2007, The politics of DDoS attacks. *IEEE – Distributed Systems Online*, **8**(8), pp. 1–3.

Gottfredson, M. R. and Hirschi, T., 1990, *A General Theory of Crime* (Stanford, CA: Stanford University Press).

Halliday, J., 2010, US report claims Chinese telecoms company had access to 15% of global traffic, including military emails, for 18 minutes. 18 November, *The Guardian*.

Harrison, M. I. and Shirom, A., 1998, *Organizational Diagnosis and Assessment: Bridging Theory and Practice* (Thousand Oaks, California: Sage).

Heimann, C. F. L., 1993, Understanding the Challenger disaster: Organizational structure and the design of reliable systems. *The American Political Science Review*, **87**(2), pp. 421–435.

Kahn, A. E., 1966, The tyranny of small decisions: Market failures, imperfections, and the limits of economics. *Kyklos*, **19**(1), 23–47.

Kemmerer, R. A. and Vigna, G., 2002, Intrusion detection: A brief history and overview. *Computer*, **35**(4), pp. 27–30.

KPTVstaff, 2010, Theft in Molalla [Oregon] reported to Department of Homeland Security: Computer controlled town's water system. *KPTV.com Homepage: Portland News*, March 26. Online. http://www.reclamere.com/index.php?mact=News,cntnt01,print,0&cntnt01articleid=268&cntnt01showtemplate=false&cntnt01returnid=27

Kuhn, D. R., 2002, Sources of failure in the public switched telephone network. *Computer*, **30**(4), pp. 31–36.

LaPorte, T. R., 1975, *Organized Social Complexity: Challenge to Politics and Policy* (Princeton, NJ: Princeton University Press).

Lindner, F., 2006, Software security is software reliability. *Communications of the ACM*, **49**(6), pp. 57–61.

Mayntz, R. and Hughes, T. (Eds), 1988, *The Development of Large Technical Systems (LTS)* (Boulder, CO: Westview Press).

Mills, E., 2010, Insecurity complex: In their words: Experts weigh in on Mac vs. PC security. *CNET online*. http://news.cnet.com/8301-27080_3-10444561-245.html

Model, H., 2000, Organizational success and failure. *European Management Journal*, **18**(5), pp. 488–498.

Nojeim, G. T., 2010, Cybersecurity symposium: National leadership, individual responsibility: Cybersecurity and freedom on the internet. *Journal of National Security Law & Policy*, **4**, pp. 119–233.

Oates, J., 2008, Submarine cable cut torpedoes Middle East access: Web slowdown hits India, Pakistan too. *The Register*, online. London. http://www.theregister.co.uk/2008/01/30/india_mideast_lose_internet/

Perrow, C., 1984, *Normal Accidents* (New York: Basic Books).

Porche, I., 2010, Stuxnet is the world's problem. *Bulletin of the Atomic Scientists. Washington, DC*. http://www.thebulletin.org/web-edition/op-eds/stuxnet-the-worlds-problem

Rheingold, H., 1993, *Virtual Communities: Homesteading on the Electronic Frontier* (Reading, MA: Addison Wesley).

Sagan, S. D., 2004, Learning from normal accidents. *Organization & Environment*, **17**(1), pp. 5–19.

Sanger, D. E., 2010, Iran fights strong virus attacking computers. *New York Times*. 26 February. Online. http://www.nytimes.com/2010/09/26/world/middleeast/26iran.html?hp

Schroeder, P., 2000, A brief history of Microsoft and accessibility. *AccessWorld*, **3**(14), p. 05. http://www.afb.org/afbpress/pub.asp?DocID=aw010402

Seltzer, L., 2010, Did China hijack the internet in April? in: L. Seltzer (Ed.) *Security Watch*. Online: PCMag. http://securitywatch.pcmag.com/dns/283695-did-china-hijack-the-internet-in-april

StaffEconomist, 2008, Of cables and conspiracies. *The Economist Online*, February 7.

Tierney, K. J. and Goltz, J. D., 1997, Emergency response: Lessons learned from the Kobe earthquake. *Emergency*, **1**. http://dspace.udel.edu:8080/dspace/handle/19716/202

Ting, M. M., 2003, A strategic theory of bureaucratic redundancy. *American Journal of Political Science*, **47**(2), pp. 274–292.

Wales, E., 2002, Your money or your website? *Computer Fraud & Security*, **2002**(12), pp. 7–8.

Wellman, B., 2002, Little boxes, glocalization, and networked individualism. *Digital Cities II: Computational and Sociological Approaches*, **2362**, pp. 337–343.

Williams, M., 2011, Blocking internet cost Egypt at least $90M, says OECD. *Computerworld*. February 3. Online. http://www.computerworld.com/s/article/9207938/Blocking_Internet_cost_Egypt_at_least_90M_says_OECD

Wohl, J. G., 1981, Force management decision requirements for Air Force tactical command and control. *IEEE Transactions on Systems, Man, and Cybernetics*, **11**(9), pp. 618–639.