Rise of a Cybered Westphalian Age

Chris C. Demchak
Peter Dombrowski

No frontier lasts forever, and no freely occupied global commons extends endlessly where human societies are involved. Sooner or later, good fences are erected to make good neighbors, and so it must be with cyberspace. Today we are seeing the beginnings of the border-making process across the world's nations. From the Chinese intent to create their own controlled internal Internet, to increasingly controlled access to the Internet in less-democratic states, to the rise of Internet filters and rules in Western democracies, states are establishing the bounds of their sovereign control in the virtual world in the name of security and economic sustainability. The topology of the Internet, like the prairie of the 1800s' American Midwest is about to be changed forever—rationally, conflictually, or collaterally—by the decisions of states.

In 2010 the crossing of the Rubicon into the age of cybered conflict[1] occurred with a surprisingly sophisticated, precisely targeted, and undoubtedly expensively produced worm in large industrial control systems. Its name was Stuxnet. As a malicious piece of software, it came as a surprise despite having floated around a year doing nothing but stealthily copying itself. The worm's target was the program controlling centrifuges in Iranian nuclear reprocessing plants.[2] Spread by infected USB thumb drives and the software in printer spoolers, it bypassed the Internet security controls in place against hackers and did not act maliciously until finding

---

Dr. Chris C. Demchak, a former Army Reserve officer, received her PhD in political science from UC Berkeley and holds an MPA in economic development from Princeton and an MA in energy engineering from Berkeley. She has published articles on comparative security, cyberspace, organizations, and large-scale systems surprise and three books: *Military Organizations, Complex Machines*; *Designing Resilience*; and (forthcoming) *Wars of Disruption and Resilience*: *Cybered Conflict, Power, and National Security*.

Dr. Peter Dombrowski is a professor of strategy at the Naval War College and chair of the Strategic Research Department. Previous positions include director of the Naval War College Press, editor of the *Naval War College Review*, co-editor of *International Studies Quarterly*, associate professor of political science at Iowa State University, and defense analyst at ANSER, Inc. He has authored over 45 articles, monographs, book chapters, and government reports and is co-editor of *Balance Sheet: The Iraq War and U.S. National Security* (Stanford University Press, 2009).

the precise computer DNA of Iranian nuclear reactors as Stuxnet's designers intended. While the worm infiltrated a wide variety of protections and Windows operating systems, the sophisticated Stuxnet authors demonstrated a new level of threat to cyber security. Despite early denials, the Iranian nuclear community ultimately admitted its plants were infected and its centrifuges unstable.

Stuxnet capped a two-year period in which the scope and complexity of national security challenges posed by cyberspace created a new level of insecurity.[3] From 2008 onward, a string of unsettling discoveries of massive theft of national data appeared via backdoors into otherwise secure national-level systems (e.g., GhostNet). Widespread stealthy infection of national systems occurred through sophisticated programs waiting to be connected to hidden remote servers, such as the Confiker worm and the wholesale copying of critical industrial technological advances by China. The age of vandals and burglars in cyberspace moved to the next level, resembling organized cyber mercenaries, cross-national pirates, and the undermining of nation-states on a massive cyber scale.[4]

Until Stuxnet, however, it was not entirely clear if all the access points, malware, and rampant penetrations would lead to serious strategic harm. The consensus among states changed after Stuxnet. If such malicious software can take down whole energy systems at once, states have no choice but to respond if they are to protect their own governmental and military operations and uphold their responsibility to protect citizens and corporations.[5] The Stuxnet method and its success thus changed the notion of vulnerability across increasingly internetted societies and critical infrastructures. The days of cyber spying through software backdoors or betrayals by trusted insiders, vandalism, or even theft had suddenly evolved into the demonstrated ability to deliver a potentially killing blow without being anywhere near the target. Forcing nuclear centrifuges to oscillate out of control from an unknown and remote location suggests that future innovations might be able to destroy or disrupt other critical infrastructures upon which modern societies depend. As proof of concept as well as a model to be copied, the Stuxnet worm offers the possibility of distant enemies spending hundreds of staff hours and expertise to insert such applications throughout the nation—from oil pipelines to dam turbines to nuclear and fossil fuel energy plants to any other large-scale critical service controlled by computers. As the designers of Stuxnet demonstrated, being disconnected from the Internet will never again be a guarantee of security.[6]

If any part of the plant, service, aircraft, or system is internally connected or if any electronic devices connect to the system from the outside, even if the device must be hand-carried, the system is vulnerable.

Stuxnet is an exquisite example of the advantages afforded attackers in the current global cyberspace. Attackers freely choose the scale of their organization, the proximity of their targets, and the precision of their target group, all with near impunity. They may take all the time they need in capitalizing on these advantages and in using the Internet itself to collect more data on the intended targets. The ease of relatively risk-free conflict between adversaries within the global web is so apparent even bot net gangs of criminals controlling secretly hacked personal computers fight among themselves technologically, often seeking to destroy and replace the other's malicious software. As shown by the denial of government and banking service in Estonia in 2007, wholesale assaults across physical borders can be deployed from one state to another by "patriotic hackers," while the originating state claims ignorance and inability to stop the assault.[7] By 2008 alone, the daily attacks on simply the US ".gov" or ".mil" websites numbered in the millions.[8] Over the course of 2009, an unprecedented 75 percent of global companies across 27 countries were the victims of cyber attack, with the average reported loss of $2 million.[9]

Today, protective measures in modern democratic states are often insufficient to repel the daily onslaught of attacks by state and nonstate actors, and the situation is worsening. Stuxnet's success ensured the rising perception of an all-source 24/7/360-degree national-level threat. In the future, a "son of Stuxnet" variant could also float for some time, seemingly harmless and unnoticed until triggered by a particular date, end-use, Internet signal, or an encounter with a specific kind of computer or program. At once, millions of computers might fail, suddenly try to send destroy commands to countless others, or even worse, suddenly replace true data with false in anything from aircraft to mass financial transactions. Even China recognizes an internal threat from its own vigorous development of cybered hacking talent inside the nation. While the intent had been to use the skills outwardly in "patriotic hacking," despite severe sanctions against hacking Chinese citizens, now Chinese authorities have to contend with their own very real internal cybered threats.[10] States under such constant barrage cannot help but respond.

All states, in one way or another, will reach out to control what they fear from the Internet—the lack of sovereign control over what comes through

their borders. Thus the transformation from frontier to regulated substrate across cyberspace has begun. While it is not recognized as such nor publicly endorsed by most democratic leaders, a cyberspace regulating process is happening, building the initial blocks of emergent national virtual fences. A new "cybered Westphalian age" is slowly emerging as state leaders organize to protect their citizens and economies individually and unwittingly initiate the path to borders in cyberspace. Not only are the major powers of China and the United States already demonstrating key elements of emerging cybered territorial sovereignty, other nations are quickly beginning to show similar trends. From India to Sweden, nations are demanding control over what happens electronically in their territory, even if it is to or from the computers of their citizens.

This process may be meandering, but we argue it was inevitable, given the international system of states and consistent with the history of state formation and consolidation. As cyberspace is profoundly man-made, no impossible barriers hinder the growth of national borders in cyberspace. They are possible technologically, comfortable psychologically, and manageable systemically and politically. Small steps in securing against threats will lead to further steps over time and, especially, in response to discoveries such as Stuxnet or its derivatives in the future.

In the process of border development, the singular marker of a new age of sovereignty and cybered conflict will come to be a normal part of the modern state's capacities: the national cyber commands or their security equivalents at the national level. To assure national safety in cyberspace, large, vulnerable states like the United States and China must anticipate and disrupt attacks far forward as well as repel a wide variety of threats. Otherwise, the mass attacks may spread too fast for effective defense. Just as militaries still exist in the modern age of mass weapons, they or their functional equivalents will also be sent to guard key national points in cyberspace. In so doing, they deepen national borders. This article argues Stuxnet marks the official beginning of a new cyber Westphalian world of virtual borders and national cyber commands as normal elements of modern cybered governments. Finally, we have seen these kinds of phenomena before in the old Westphalian world. Already, theories, international rules, institutions, and experiences exist to guide us as the new age fully matures.

The "Westphalian" Process

The Stuxnet worm marks a turning point into a new cybered conflict age in which states need to define territorial spaces of safety to reassure their citizens' safety and economic well-being. When it is widely accepted that critical systems can no longer be trusted if they are open to the web, political leaders will demand ways to eliminate the threats from entering their territory. The cybered conflict age has begun, and it is natural for those hostile to any particular group to include cyber at key points in their plans, including debilitating entire systems. Equally expected, leaders of the threatened group will have to consider what responses keep critical functions secure. From water holes in the desert to river passages in the forest to mountain passes to central controlling nodes in the global web, conflict parties inevitably seek the critical gateways of the opposition to obtain advantage.

Frontiers are places of conflict between groups, historically lightly and poorly governed, less populated, and risky—places where value is extracted for little cost. When a frontier starts to become a commons, productivity for all is imperiled by the grab-and-go nature of those using it. Those dependent on the frontier tend to form organizations to control their claim. Modern democracies are in essence complex aggregates of large-scale organizations. Their leaders routinely reach out to absorb uncertainties to control them, if possible, or push them away.[11] The rising perception of a national-level threat means that all states, in one way or another, will reach out to control what they fear from the Internet—its frontier nature and the lack of sovereign control over what comes into their area of responsibility.

No freely occupied commons extends endlessly nor lasts forever where rising rapacious human populations are involved. It is normal for political leaders seeking relief from the interaction edges with other cultures or possible threats to look at reinforcing or installing borders. Being able to establish sovereign control is one hallmark of a functioning state. This need is true whether the border is enforced by passports for people, customs inspections for goods, or two-way filters for meta-tagged electronic bits. When states cannot protect their economic engines of growth and sustainability, the capacity of the state falls into question by those who control the resources under threat.[12]

Man's search for security has led to the formation of "fortress and badland" distinctions that marked territory for resource ownership for centuries, but

until the 1648 Treaties of Münster and Osnabrücke (understood together as the Peace of Westphalia), borders did not stabilize over many generations. In this particular case, however, the Peace of Westphalia not only ended the Thirty Years' War in Europe but also heralded the emergence of the modern interstate system. After the Westphalian peace, the nation-state became the dominant form of social organization. As a result, leading states of the period helped codify and set about more or less enforcing a collectively agreed upon set of rules, institutions, and norms by which they interacted with each other in international society.[13]

Particularly useful for international stability was the effect of the treaties in creating conditions supporting the gradual hardening of borders between and among states, more or less, over the next 362 years. This process of settling on boundaries due to the mutual adjustments among states produced a concept of national territoriality that states could legitimately claim, and they could defend that territory against outside aggressors in just wars. With the rise of a general presumption of territoriality recognized by other external political leaders, modern states were able to stabilize internally and grow economically within those established, increasingly fixed borders.

Westphalia provided a demonstration or a proof of concept. Over time, the more established a state became and the fewer ungoverned internal areas or frontiers it allowed to continue, the stronger and less existentially vulnerable the nascent state became.[14] The significance of the Westphalian process for this article and its general argument is that the efforts of the modern state to cope with the emergence of the cybersphere is in many respects similar to the processes by which states became the dominant form of social organization within the international system. The ability of the state to provide stability and security within the increasingly unchallenged borders was necessary to internal development of social and economic progress. Without a form of Westphalian borders, conflicts previously at the boundaries easily spill over in both directions from opportunistic resource appropriations by actors within and without. The wide variety of authorities, powers, and capabilities over the last 400 years accruing to the modern state become difficult to employ, redirect, or even limit. Just as the ability of modern bureaucratic states to corral resources productively drove other less successful organization forms from the scene internationally, their ability to provide internal certainty in their domestic territory gradually

came to define what is today known as civil society in the Westernized world.[15]

Today the uncertainties, predatory and productive opportunism, legal and illegal resource conflicts, and changes to economic and social expectations reach directly into the domestic structures of the modern state. Just as before the Peace of Westphalia and its recognition of the systemic economic threats of insecurity within societies, states are beginning to grapple with the difficulties inherent in incorporating a new set of technologies into their citizens' community and individual interactions. In particular, the cybersphere has challenged the security of individuals and states themselves in ordinary systems considered essential to the critical functions of society. Increasingly, citizens are at the frontlines of the existential fight over stability in the wider society, and the responses from modern states have only now begun to crystallize.

The struggle to move these conflicts from the existential realm directly harming citizens to some more organized field of dispute has begun at least in discussions among allies and in international communities, but the process has been meandering.[16] Initially surprised by the reach of the predatory behaviors made possible by cyberspace's unfettered global reach, democratic governments have been slow to reinforce their monopoly of violence over external threats entering their nations and harming citizens. Laws emerged over the early 2000s focused on the internal symptoms rather than the external sources of the uncertainties, many focused on the individual citizen or commercial Internet service providers (ISP). For example, in the United States, financial liability to the individual defrauded online in credit card usage limited the amount the citizen would lose.[17] In contrast, German law makes individual citizens responsible if they do not stop their personal computers from being taken over and used in massive spam or denial-of-service attacks.[18] Australia, however, enforces rules on the ISPs to keep the flow of malware to a minimum.[19]

Despite these efforts, organizations and governments have found their presence in cyberspace vulnerable to attempts to extract information, prevent access, and even to disable as happened with Stuxnet. In March 2010, a US cyber security report stated the monthly number of attacks on the US Congress and government agencies had reached 1.6 billion, largely from outside US borders.[20] Governments, like the signatories to the Peace of Westphalia, are increasingly aware of the potential losses if hostile, curious, or just rapacious outside actors are able to reach easily and deeply inside

their societies, into critical assets of families, banks, townships, airlines, or any of the myriad of critical systems sustaining the society. "It appears we can no longer see the Internet as a friendly shared resource and that strict boundaries will have to be put in place," said Bert Hubert, founder of Dutch-based software provider PowerDNS.com.[21] States, especially large, often cyber-targeted nations like the United States, are recognizing the need to respond. Their efforts to control are accumulating across the organizational and technological capabilities. The modern state intends to put in place a buffer, a bulwark, a way to buy the nation time to respond if attacked. In short, they are iterating toward national borders in cyberspace to relieve the pressure of the barrage of assaults.

Practical Reinforcement—Borders Decrease the Ease of Cybered Offense

Beyond the return to interstate protocols that are well understood, there is a practical aspect to cyber borders—they make it more difficult to cause harm. Making it necessary to get around borders physically forces larger organizations of people to arrange a physical entry to each nation under attack. Forcing attackers and criminals to move people rather than bytes means higher operational barriers to entry: more costs, more coordination efforts, and many more opportunities for any of these efforts to be noticed by national security monitoring organizations.[22] The border hurdles also can slow the pace of regrouping from failures or redirecting to capitalize on new information, as well as coordinating simultaneous target groups across borders.

Increasing the organizational difficulties for attackers also increases the loyalty challenge for bad actor organizations trying to control human agents at distance rather than merely reprogramming pawned computer networks. The job of attacking civil societies increases enormously when information must be verified in situ by informants who may or may not be trustworthy dispersed across monitored virtual borders. Borders reduce the advantages of scale, proximity, and precision an attacker has in pitching offensive surprises and levels the playing field for the defending societies. Some mass attacks that are possible today may, with borders, simply become impossible unless the organization is able to physically move large numbers of humans into each targeted country and coordinate rapidly around national borders or collaborating regional institutions. Borders

raise skill, social, resource, and distance barriers for the vast majority of today's hackers and would-be attackers who lack exceptionally advanced skills.

Virtual Borders—Feasible, Comfortable, and Manageable

The slow development of a Westphalian-style accord parsing cybered sovereignty has every chance to proceed and eventually succeed. There are few natural dampeners to a neo-Westphalian process in the digital era. A cybered national border is technologically possible, psychologically comfortable, and systemically and politically manageable. Increasingly, the exceptionally skilled technologists are arguing for separation of critical systems to protect them from Internet predators and hostile actors. As a result, even if policymakers in each nation are inclined normatively to keep a fully open Internet, they will have few technical arguments to use in maintaining that position. Furthermore, borders are psychologically normal for citizens focused on continuing their access to Internet services safely. Users already expect some kind of government sanction against those who harm individuals via cyber means, and borders make historical and cultural sense for denizens of modern states.[23] Finally, a cyber border fits more easily with the institutional compromises and allocations of responsibilities already existing in the governance structures managing modern democracies.

First, the technology of cyberspace is man-made. It is not, as described by the early "cyber prophets" of the 1990s, an entirely new environment which operates outside human control, like tides or gravity.[24] Rather, as its base, the grid is a vast complex system of machines, software code and services, cables, accepted protocols for compatibility, graphical pictures for human eyes, input/output connections, and electrical supports. It operates precisely across narrow electronic bands but with such an amalgamation of redundancies, substitutions, workarounds, and quick go-to fixes that disruptions can be handled relatively well as long as everyone wants the system to work as planned.

However globally interconnected, cyberspace is dependent on preventing its internal need for precision being hijacked or massively disrupted by malicious or hostile actors. States are learning that everything about today's grid can be technologically regulated. There are many points of opportunity for the national government interested in controlling what

eventually ends up being received on Internet desktops, laptops, mobile devices, or even independent appliances in homes and businesses. While connectivity is global—now increasingly found everywhere like land, air, sea, and even space—what is known as cyberspace *is* and *will* remain always man-made, -sustained, and -enabled. And, unlike the sea, land, air, or space, it can be unmade. Furthermore, land expanses, seas, air, and space quadrants do not exist only if information is flowing. Seeing a mountain does not automatically connect one individual to the next or even offer one useful clues about it, yet being on one node does connect individuals to others in this cybered underlayment, even if only with some hacking. Air masses are air masses, but strings of cyber bytes already have information in the way they connect from node to node in protocols. It would be as if a car could not continue on the freeway without broadcasting its VIN number, license, weight, and other data each time it approached an exit. If not approved to continue by the owner of that freeway node, the car would be forced off onto another road.

Today, someone and some firm or agency built or bought now runs and must maintain every single connection on the Internet. Even peer-to-peer (P2P) networks require a person to connect and maintain them. Some firm must develop the software to allow connections, and someone must also code the application allowing the exchanges of data, for good or ill. Today the technological filtering occurs largely through private or semi-private institutional intermediaries. Across the bulk of democratic and nondemocratic states, ISPs are finding their ability to continue to provide services is increasingly dependent on providing filtering services determined by large, state-level authorities. There is no technological reason why these services cannot continue as regulated utilities, nor is there any reason why governments cannot control what runs into the nation from overseas cables or runs out of the nation to criminally harm citizens of other nations.

It is technologically possible for governments to require source tagging of bytes at some point to assure the passage of legally acceptable streams of data or applications or volumes of requests as a way to curtail attacks on their soil or emanating from their soil illegally.[25] Changing the mix by social accord via government action changes the system as we access it, know it, and use it. If key cable junctions are broken, the Internet fails or slows to a crawl for whole nations. If the same cables are merely redirected through an extra set of computers which reject or delete unwanted patterns

of data, then the Internet at the far end of the redirect will seem to be all that it was. Deleted material will simply never show up. With sufficient investment in leading-edge speed cables, inserted filtering servers, and capable transmission lines, it is possible to have a border that is not visibly intrusive to the vast majority of citizens and conceivably even faster than today. For example, while it is widely known China controls its Internet, it is not widely known that this control rests on having only three main Internet gateways between its one-billion-plus population and the rest of the globe.[26] For the kinds of controls exerted by the Chinese government to go unnoticed by users is one piece of evidence that a border for every state, each with different security goals, is within technological reach, if not yet legally and formally sought.

Second, physical borders are known, accepted, and desired by citizens in modern civil societies, and that psychological comfort will be no different for the creation of borders in cyberspace. The relevant emphasis is on "borders," not on universal control of all cybered transactions occurring entirely within the boundaries of a democratic nation. Historically, citizens accepted borders as a security-enhancing necessity against external uncertainties undermining internally accepted rules of interaction. Without such limits, the collective sense of belonging is more easily undermined, as are the rules of civil behavior. Even a willingness to abide by norms of trust and nonthreatening behavior is tied to security, where collective rules can and cannot be enforced. To live in ungoverned societies is not only insecure; it is also a psychologically palpable existential threat. As Joel Brenner explains,

> Constitutive rules define the structure of a given society, as well as the relationships that exist among the individuals that comprise that society; they also allocate essential tasks among the members of the society and ensure that these tasks are performed. Human societies have consisted of bounded systems situated in a delimited spatial area and composed of a defined populace (e.g., "the people of Rome," "the American public," and so on). These spatial and population constraints facilitate the operation of the constitutive rules: spatial and demographic isolation make it easier to socialize those who populate a society so that most accept and abide by its constitutive rules. They also make it easier to identify and suppress those who do not.[27]

Civil society deepens and strengthens when the expectation of modern liberal and universal social rule observance is justified routinely. Historically, the hostile or predatory deviations from actors outside the social jurisdiction of a modern state is exactly what citizens in their implicit social

contract seek to avoid in according a territory their allegiance and legitimacy. Safety at home for the citizen in a highly digital society is a social-psychological need obliging the modern democratic state to act.[28]

Third, borders fit institutionally into the existing architecture of national systems management. Most nations make a distinction between the forces defending the borders from attack (militaries) and those protecting the individual citizens inside the nation from attack (police). This distinction is one of the direct outcomes of the rise of the modern state from the Westphalian Peace. But it is severely challenged by the unfettered character of the current global cyberspace topology. Today militaries, police, and intelligence organizations in particular have been challenged both by the attacks and by the jurisdictional lack of clarity in obligations and ability to demand resources. Both state and nonstate competitors have used the interconnectivity inherent to the web to attack and disrupt operations and gather intelligence about capabilities and intentions across borders with impunity. This is especially true for the United States and other nations highly dependent on telecommunications for command and control; intelligence, surveillance, and reconnaissance; and the management of logistics. Moreover, many military and intelligence organizations have grasped the offensive possibilities of the cybersphere to reach past the borders of other states directly, in concept at least, into the homes of an opposing state's citizens. Across the military communities of the more modern states, information operations and strategic communications programs have been developed to influence adversaries and allies. Physical or "kinetic" attacks are now routinely facilitated by efforts to exploit enemy cyber vulnerabilities.[29]

Without the legitimating and bureaucratic clarity of a virtual border, for example, jurisdictional disputes in nations observing centuries of criminal versus national security civil society laws are hamstrung to respond. Stuxnet easily crossed borders as intended by its designers. If it were a nonstate actor, then the action is criminal, invoking the powers of police forces. If it were a state-level actor, then militaries would be involved. Today it is not clear which groups were involved, in large part because the electronic trail of possible attribution moves readily across states, and states have no obligation to sanction bad behavior emanating outward from their territory. Nonetheless, a state's facilities were harmed, and many states are viewing that uncertainty and inability to lay blame and attribute the attack as unacceptable vulnerabilities.[30]

In principle, only from ungoverned or ungovernable territories do modern groups launch destructive missiles on neighboring nations without automatic interstate calls for sanctions. With physical borders, states that wish to be accepted internationally are obliged by law and custom to stop the attacking behavior of their residents or to allow the offended state to reach inside to stop it. Once the virtual limits of sovereign power can be demarcated in the global cybersphere, states ignoring or supporting massive denial-of-service attacks from their territories will be held internationally responsible. Domestic legal systems that today do not have internal laws criminalizing predatory cyber behavior affecting other states will have to initiate the kinds of internal controls already presumed in international policing. If they do not or if they actively promote the external attacks from their territory, just as in centuries of physical conflict, they will have to acknowledge the right of the attacked states to defend across borders if necessary. Distinguishing criminal laws and activity from national security missions and jurisdiction becomes enormously more manageable when the jurisdictional lines are drawn and recognized in a new cyber-Westphalian process.

Managing the bordered virtual sphere will also enable a third swathe of cyberspace to be identified as well—the ungoverned badlands equivalent to the very physical regions of failed or failing states. As civil society extends into cyberspace with rules of accepted behavior and reinforced by modern state institutions, it becomes easier to invoke the routine activities of international organizations to curb, if not cure, the disruptive activities of the failed-state portions of the international virtual globe. As a result, institutions will adapt and adjust while replicating the functional aspects of the current physical concords and rules of behavior to contain the harm by actors who deviate from the emerging virtual civil world. What is happening today in the slow civilizing of cyberspace, however scattered and seemingly unique, strongly depends on what individual governments see as either the threat or the leverage they have and the institutions they develop to act on those perceptions. For all, the beginnings of a need to control the sovereign, albeit digital, national territory is already present. None are controlling the harm, transmission, laws, or sanctions emerging on the sovereign territory of another state; rather, each is operating under the modern notion of monopoly of power on the territory already demarcated and looking to its own laws and control of actions on its territory, to include network connections.

Emergent Virtual Borders

Indications of emergent borders within the cybersphere are appearing at many levels, making for a variety of models across the current extent of sovereignty the state presumes or seeks. So far some are quite singular. China leads the authoritarian states in a more ubiquitous cyberspace regulation model aimed at controlling information from outside and circulating inside its borders. In this "all points" model, the border boils down to gateways largely filtering information with the ability, in principle, to curtail the Internet connections, either between internal regions or between China and the rest of the world. It is a technological (limited gateways), institutional (regulated telecoms), and psychological (cyber self-censors and vigilantes) model operating on many levels at once.

In this model, China is expressing a long-standing concern for the stability and security of the well-established Chinese territory. "Whether we can cope with the Internet is a matter that affects the development of socialist culture, the security of information, and the stability of the state," President Hu of China said in 2007.[31] In the 1990s, the Chinese Communist Party recognized the power of unfettered access from/to Chinese citizens and declared the Internet to be a fifth area of territoriality to be nationally secured. They built the "Golden Shield" that employs an estimated 40,000 Internet police who in 2009 shut down about 7,000 websites, deleted 1.25 million pieces of information, and arrested 3,500 people, including 70 dissidents and bloggers now in jail. In addition to directly controlling the content, about 30,000 netizens are employed part-time to intervene in online forum discussions and redirect conversations away from sensitive topics. The Chinese leadership routinely characterizes Westernized social media as subversive tools and sees the hand of the United States in diplomatic subversion in any US–sponsored discussions of open Internet. With the view that state security and social stability are under attack, the Chinese government implemented the strong, technologically sophisticated, heavily intelligence collection–driven second phase of the Golden Shield in 2010.[32]

For at least six years, China has also been working on constructing its own Internet. In what is called China's Next Generation Internet (CNGI), the current limited number of Internet addresses expands massively by adding enough digits (IPv6)[33] to provide every single machine connecting to the Internet its own unique web address. This addressing protocol also means every single web transaction can be tracked from the original machine

to any other, allowing a massive societal control advantage when linked to other rapidly emerging advances in the raw computing speed and storage of computer systems. Not only will three-dimensional online worlds move faster and more realistically, but also every interaction in those worlds can be recorded or individually tracked in real time to the specific machine.[34]

A new, more surveillance-friendly addressing system is useful to the Chinese or any government desiring to control its own borders without having to use proxies or agents to do their controlling. The so-called Great Firewall that Google declined to support in 2010 was in reality the imposition of liability onto ISPs if one of their users accessed forbidden sites or topics.[35] As Google demonstrated, this "intermediary liability" approach to control has its limitations for a nation known to have a cultural preference to avoid proxies.[36]

The justification of these measures as essential for citizen safety against social disharmony, false information, fraud, piracy, and social ills such as pornography is a common theme in the oft-times bumpy path to creating a sovereign border in cyberspace. For example, in 2005 the Chinese announced an upgrade to the national text messaging filtering system with automatic police alerts when false information, reactionary remarks, or harmful activities such as fraud and scams are found in cell phone texts. In December 2005 the vice-minister of the Ministry of Public Safety announced that the upgraded system's 2,800 surveillance centers had tracked about 107,000 illegal cell phone text messages in November 2005. With about 33 percent of the texts associated with criminal fraud activities, 9,700 cell phone accounts were shut down over the month.[37] At the time (2004), Chinese citizens annually sent 218 billion text messages, against which an objectionable number of 107,000 is not even a drop in the bucket. By 2010, however, the addition of supercomputers which can move trilobits per second provided advanced capabilities to filter cell phone text messages centrally. The police, using undisclosed criteria, create lists that cell phone companies must use to scan all customer text messages. Companies must automatically suspend the accounts and report the incidents to police if banned terms are found.

The new technologies have enabled not only massive increases in the intrusive and comprehensive search mechanisms but also more punitive measures against those found to violate the restrictions. During the same period of slowly gaining control of all communications media, the Chinese authorities have closed websites, especially those able to share files, and

increased the difficulty for citizens to have their own sites.[38] Already the Chinese government has channelled the physical access of all web traffic in or out of China through three major gateways in Beijing, Shanghai, and Guangzhou.[39] Whether or not the international community approves, China's government is engaged in using the accretion of internal controls on content as a consistent part of a state asserting sovereignty over key aspects of its internal social territory.

Several democratic nations have charted a "key firm" model of regulating the large telecoms, albeit loosely, with the goal of curbing malicious or thieving activity, not information flows. These include Australia and to some extent Germany. Major Westernized, largely European democracies are enacting or strongly considering enacting Internet control measures to prevent theft or abuse of their citizens' personal information and the economic assets of their countries. Others, such as the UK, turned initially to pan-agency coordinating economic or social, but not security, institutions to encourage, monitor, and guide internal Internet transactions. The goal is to curb foreign and local theft of national economic assets and private personal information. More recently, however, even European nations have shown an increasing tendency to see a role for national security controls, although less prominently discussed. In 2008, Sweden passed legislation allowing its national police force's intelligence section to monitor all Internet traffic in and out of the country, whether by Swedish citizens or others. It was challenged widely and loudly by prominent privacy advocates, but the law withstood challenges as a central piece of anti-terror legislation and was institutionally implemented in late 2009.[40] The model is still firm based but is increasingly more focused directly on security.

The path to a national border in cyberspace may not prove as difficult for EU nations as it would for other sectors because cyberspace policies are currently left largely to member states. The level of security varies greatly across nations, and it is unlikely the UK will, any more than France, wait for an EU–wide solution to threats to its own cyber resources or citizens.[41] The UK, in particular, has moved incrementally to lay the foundation for a national border, sometimes for political reasons having little to do with cyberspace, such as a national identity card to curb illegal immigration. The rise of serious intrusions into sensitive government networks—at least 300 over the course of 2009—has pushed the island state to construct two agencies with the specific missions of coordinating and informing the tools, tactics, and targets of cyber security across all governmental

agencies.[42] Current trends suggest the UK will be closely behind the United States over time as the elements of a national border in cyberspace are erected, in large part because the UK, as a close partner of the United States, is both more of a target and more informed about its vulnerabilities than other EU nations.

The singular marker of an emerging border, however, is the creation of a military organization—a cyber command—to protect the nation from the kinds of harm that historically only a peer state or neighbor could inflict. For a nation to establish such a unit and publicly declare to have done so, that state is explicitly saying it has territory to defend and the threat to be met poses conceivably an existential threat. Such a unit marks the acknowledgement of a nationally owned space that the nation values and will protect using available and appropriate resources, including regulatory, law enforcement, and military capabilities. That the borders have not yet been recognized by other nations—a key outcome of the long Westphalian process—does not diminish the significance of this institutional declaration of sovereignty to be defended, by definition, in cyberspace itself. While not as advanced as either China or Australia in controlling their domestic Internet access or policing its key industries, the United States in establishing its new US Cyber Command has laid the cornerstone necessary for a national cyber border. The nation has stated an intention to defend against, repel, or prevent whatever could come across its cyber border and do so with its military might and resources if required. The declaratory aspect of this unit is important as a permanent symbol of a new cyber–Westphalian international system. China has government organizations with what Western observers presume are the same missions as Western cyber commands, but they are not publicly named as military defenders of the nation. The "cyber command" model primarily rests on the use of national security institutions for cyber defense at and beyond a border.

Cyber Command—The US Model

In the fall of 2010, the US Cyber Command became operational after an exceptionally rapid year of institutional and legal preparation.[43] This institutional response to the rise of the cybered conflict age emerged to anchor a future cybered border for the whole nation. Its initial mission was to protect only military organizations from cyber attack, but as soon

as a military unit existed to create a cyber safety wrapper around US critical military assets, political statements emerged about creating the same protection for the whole nation.[44]

From the RMA to net-centric warfare, the United States has a history of providing new models for national-level security organizations, especially military organizations.[45] For the United States to announce a new national cyber command automatically provokes a new debate in the international military and legal communities.[46] Whether or not other nations need, want, or can afford to have a singular military unit focused on cybered conflict, their leaders, doctrine writers, and strategic thinkers will contemplate whether they themselves need such a unit when the remaining superpower signals how critical it is for national security.

If patterns of military emulation occurring since World War II hold true, the vast majority of nations will inevitably have something that looks and acts like a national cyber command, whether or not it initially bears that name. Already we have seen nations closely associated with the United States either mirroring it in creating their own cyber command or declaring an interest in having a unit that approximates the functions of US Cyber Command. South Korea, for example, now has a military cyber command after enduring a massive assault in early July 2009.[47] In recent strategy discussions, the United Kingdom, while focused on the cyber protection of the entire society, has begun discussing closer integration of its military cyber resources with its intelligence cyber resources and the challenge of knowing when to use offense versus defense when a threat emerges.[48]

Importantly for the emergence of borders in cyberspace, the US model of a national cyber command has several distinctive elements. First, the unit chosen by national leaders as their initial foray into strategic national security in cyberspace was a military, not a civilianized, internal security agency built for disasters or crime. With the weight of US resources to dedicate to a strategy of purely defensive mitigation from cascading surprise attacks, policymakers chose a natural experiment that clearly reinforced the idea that simply waiting for the attacks to hit and then mitigating the effects inside the physical borders is likely to be devastatingly insufficient. Militaries operate at the edges of nations in the modern state or deployed forward to prevent attacks. Choosing a military to be primus inter pares in cyber security also reinforces the seriousness of the existential threat, as these institutions are historically the last resort of national

survival. Creating US Cyber Command has redirected much of the global conversation about cyber security from merely blunting attacks after they arrive to repelling or disrupting the attacks before they cumulate into great harm. If cyber security is a mission involving military-like actions repelling attackers, then borders will have to be determined to guide when and where these actions can occur.[49]

Second, while the mission of the US Cyber Command is currently to protect US military cybered interactions, the structure of the new command is clearly intended to blend operations to benefit simultaneously from what was traditionally considered offensive and defensive cybered operations and the collection of global intelligence. In cybered conflict, the offensive advantages of the attacker lie in relatively easily attained preemptive surprise using the intrinsic difficulty of predicting cascades in globally large-scale complex systems. The result is that a good defense requires the ability to successfully operate offensively, knowledgeably, and rapidly to preempt the preemptive attack, or at least anticipate it with sufficient time to prepare and mitigate its effects. The peace versus war distinction has very little meaning operationally in the current frontier-like nature of global cyberspace, and the US Cyber Command model directly acknowledges the loss of this strategically and internationally accepted distinction by dual-hatting its commander as the head of the premier electronic intelligence agency, the NSA, and the military commander of the new cyber command.[50] In that Hobbesian choice, the blend of intelligence and a decision to act offensively occurs in the internal deliberations of one man subject to national laws but able to act quickly and knowledgeably if necessary.[51]

That the cyber command has the ability to attack, defend, and collect information globally is an innovation critically important not only for the United States but also for the wider international community resolutely tied to seeing conflict and peace as distinct. While the concept of a Cold War or an international crisis is routinely understood and used in characterizing disagreements, war is distinguished from peace to clearly politically and psychologically guide international institutional actions, negotiations, and strategic expectations. Unfortunately, cyberspace by its dual-use nature and ubiquity can be simultaneously hot, cold, warm, or turbulent in different parts of the world. The US innovation made it clear the last superpower thinks security rests on acknowledging that emerging reality with a unit commanding serious attention by would-be attackers.

Put differently, the model demonstrates a conclusion—that offense, defense, and extensive knowledge collection are needed to be secure—and a hypothesis that the best way forward is to build on the already organized structures of a military. For the vast majority of European democracies which have a great deal of difficulty in publicly and politically endorsing offensive measures in cyberspace, cyber security institutional adaptations have been incremental, mired in lengthy debates on civil liberties and economic progress threats. The exceptionally rapid implementation of the cyber command model by the United States has broken the allies' collective cognitive logjam. Now, whether or not senior leaders agree in principal with the solution, they are discussing new organizations and responses for repelling a threat capable of existential damage; not just burglary or theft, but massive undermining of the economic health of the state. The developments of the Confiker worm, widening ravages of international cyber crime, and lastly the unsettling discovery of Stuxnet and its success in a critical infrastructure have sparked a strong new interest in the US model, at least as an alternative.

Becoming more widely accepted is a growing national need to consolidate the efforts of the state for protection against an extraordinarily complex set of possible hidden, lightening fast, and massive threat avenues. It occurred to every successful medieval leader that one needs moats, walls, watch towers, and guards, but also one must have rapid-reaction horse- and/or ship-mounted units to keep the worst attackers far from the capital. A national unit blending all those age-old functions in cyberspace becomes a logical consideration.[52] Within a year of constructing two distinct units for cyber security—one at the Cabinet level—the change of British government in 2010 resulted in a stronger link between these units and budget increases for cyber. Furthermore, the new government declared cyber threats to be a top-tier national security issue.[53]

Similarly, in late 2008, France published the first defense white paper since 1994 and not only added the concept of whole-nation security but also elevated cyber security to one of four key national threats. The mission was to create an institution capable of guiding the other agencies in protecting the entire nation's national cyberspace. In the process a small, formerly secretive organization has become its central and publicly discussed Agency for National Information Security (ANSSI). Over the course of its first year of existence, 2009–10, the organization has helped research and justify legislation to allow further central control of defensive

and, if necessary, offensive national cyber means.[54] Other nations, especially those with limited cyber resources such as the Baltic States, are notably pushing strongly for NATO as a military organization to be designated as guarantor of their national cyber security, especially if cybered means accompany physical assaults to undermine the nation's resilience.[55]

Third, by making US Cyber Command across rather than separate from the four military services, the new organization carries within it the seeds of its future elevation in importance for the nation. As concepts for repelling attacks aimed beyond military forces at the heart of the United States have begun to coalesce politically, critical practical decisions will be made about where the tripwires are to be virtually drawn and maintained. The model does not make a small unit that simply supports other government actors in the military. Rather, its size, prominence, and position atop subordinate service-only cyber commands reinforce the universality and possibly existential importance of the task to the whole nation beyond the .mil community. All the services are involved, and all of them are required to contribute to a coordinated national response to a major event involving US military elements. Only a few threats—such as nuclear war and terrorism—have forced such rapid, unequivocally collective and ubiquitous responses beyond traditional physical domains of land, air, sea, and space.

Recently, a memorandum of agreement between the US Department of Defense and the Department of Homeland Security (the lead agency for national cyber defense for government agencies and critical infrastructure) formally initiated a process for the DoD to aid the DHS in the event of cyber-related catastrophes. The memorandum clearly invoked the direction of the support from the cyber-saavy DoD (read NSA and US Cyber Command) to the cyber-responsible but overwhelmed DHS.[56] In this, another step is taken toward a national notion of a cyber territory to be defended, a virtual space involving the whole of the society. The terms of crossing over from border and outward duties for the military to inward, more-domestic missions as a function of an anticipated cas extremis underscores both the importance and the need to have identified the border itself to regulate these agreements.

Fourth, the offensive operations mission of any cyber command working for a democracy underscores the need for other democracies to establish their own borders in cyberspace to demand noninterference in practice as well as de jure. The US Cyber Command model leaves unanswered the question of bad actors operating from within one democracy operat-

ing outward to harm other democracies. This lack of clarification of the precise operational rules of engagement and reach was left unresolved in part because the debate on that legal authority alone could have stalled the creation of the cyber command and the defense it provides.

Leaving the debate open to discussion with allies and other democracies allows for parsing out the actions of allies, especially in NATO. Experience will channel the next range of evolutionary steps for all concerned, but there is an unspoken presumption, especially among senior NATO partners, that Western democracies in particular are united in wanting security in everyone's cybered systems. Nonetheless, while the United States is unlikely to see its new cyber command as threatening allies, that benign assessment is not universally shared. Many parties on the left in many European states are routinely concerned, with good historical reasons, about the concentration of power in government hands. For example, Germany is creating a centralized cyber-crime facility that would support de facto if not de jure an emerging all-source cyber-crime service. The facility will be built, but the unified analysis seen as key will not occur among permanent cadre due to Green Party politicians' fears of concentrated data on citizen actions being in the hands of the federal government. As a result, the facility will be more of a repository that individual agencies may consult as needed. The deliberate dispersal of organizational interaction defeats the concept intrinsic to an organization such as US Cyber Command or, for that matter, a centralized cyber security operations center (CSOC) as set up in the UK.[57] This fear, however historically justified and currently endorsed, is more likely to view the US development of a virtual border with skepticism and some concern with the extent that a military cyber command is attached. In particular, they are likely to be more interested in a border in cyberspace for their own nation to have the ability, if necessary, to constrain US government actions in cybered preemption that are anticipated to harm European citizens.[58]

At the end of the day, both friends and enemies will be further incentivized to consider their own ability to demarcate in boundaries and defend in institutions their own national slice of cyberspace.[59] Creating US Cyber Command is only one mark of transformation, but it further accelerates the state-level interest in acquiring greater control of the uncertainties of the rapidly declining cyberspace frontier. This transformation is not only natural for the new cybered conflict age, it may be desirable for a future

civil global society still interconnected but with international rules guiding interactions.

Resuscitation of International Relations Theory and History

With the establishment of borders in cyberspace, everything we know about deterrence, wars, conflict, international norms, and security will make sense again as practical and historical guides to state actions and deliberations. With a border in and enforced by technological means, also essential will be the means to monitor who is electronically crossing the line in the virtual sand and whether that passage of bytes is permitted by national law, either criminal, civil, or national security. These means will have to be maintained and adapted to emerging new threats. These mechanisms will be a combination of encryption, unique machine/user identifiers centrally controlled, and local hardware-human "bio"-metrics. No more would the near-Herculean task of tracking bad cyber actors on a massive scale hinder a normal civil society's desire for a functioning mechanism to deter that source of harm. A border in cyberspace necessarily presumes some form of verifiable and current originating data for everything trying to pass into the nation, from bytes to malware to phishing or mass assaults. The nature of connectivity and emergence of other states means bad data which comes from someplace will necessarily come from some territory of some state with overarching responsibility for allowing such transmissions to continue. No longer can a state claim it is not harboring those attacking every .mil address in the United States while encouraging their internal development of "patriotic" hacking skills and a blind eye to those who hack outwardly only.[60]

In the bordered future world of digitized states, actual hot war will also be forced into expressions that can be recognized. Cross-border attacks will be regarded as such, even if largely cybered in their characteristics. If the sponsoring state refuses to stop the attacks or to allow the defending state to reach inside its territory to stop them, then the sponsoring state can be presumed to support them. Conditions much like the onset of war can then be said to exist. Wars albeit cybered will have all the pieces we have seen over the course of centuries, to include tensions, collateral damage, revenge myths, and arms races. We will deal with war as well as its

phases in warmth, cooling, and even termination en route to civil or at least calm relations as well as we were likely to do without the Internet.

It is not clear what alternatives exist in any case. It is far from clear that global civil society was enhanced in the world's poor or floundering regions by freewheeling access to every human pathology allowed by the two decades of the Internet. Those who benefited from the looseness already had a civil society in their national democracies and standards of decent behavior plus social norms on predatory behavior. Nor was the civil society goal of fairness and stable international development advanced by the wholesale secret extraction of technological advantage by one large mercantilist nation in particular pilfering massively and widely the industrial hard drives of other more-advanced nations. Those states whose firms and societies paid for the research and development have lost competitive advantage across their economies not only in jobs but also in basic resources on which to build future technological advantages. The communities of love and toleration envisioned by Rheingold in the 1990s did not flower save in small middle/upper–class educated communities; even social networking sites quickly developed predators, cyber bullys, and stalking. Today, even the original uptopian social chat site, "the Well," refuses anonymity.[61] It seems communities of hate, exploitation, and fraud grow as fast, if not faster, than the open, sharing, and enhancing virtual societies.[62]

With the rise of a national interest in protecting their own cyber turf, international norms will be negotiated state by state, region by region, coalition by coalition, and international regime by international regime. Cyberspace is man-made, and its commons-like characteristics can be negotiated across borders just like food production and safety, trade subsidies and streams, banking reserves and credibility, and even whaling. Life on, around, and through the virtual borders will be as turbulent, semistable, and prone to smugglers, free riders, would-be upstarts, and annoyances as the physical borders are now in harbors, airports, land crossings, and maritime lines of control. According to British prime minister Gordon Brown in 2009, "Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our position in cyberspace in order to give people and businesses the confidence they need to operate safely there."[63]

Many unique concerns of key nations will continue as well, perhaps easier to pursue when national cyber borders are consensed upon. For

example, one would expect no change in Germany's demand for national cultural reasons to close its ports to neo-Nazis and chase smuggled peer-to-peer Internet sites that encourage attacks on brown-skinned people, just as Saudi Arabia will close off pictures of women in positions of power and chase P2P porn sites and dissidents internally. The Chinese bureaucracy will refuse to agree to international constraints on its national right to execute addicted online game fanatics who commit crimes and jail those who smuggled pictures of the Dalai Lama or a real CNN headline internally. Tunisia and Libya will simply not talk about their internal controls and demand the usual physical rights to do technologically what they will. Status quo pro ante will adapt to the emerging topology across the globally connected socio-technical world.

Today, the United States has declared cyber threats to be at the top ranks of national security concerns, created a new major military unit, and moved along a multitude of fronts to shore up its own national ability to forestall destructive cybered cascades operating from cybered means. But normalcy also requires recognition of the international community's role in reducing interstate cybered threat just as borders may rise to protect a particular state. If attackers are limited by borders in the number of states they can attack at once using cybered means in their operations, they are forced to forage for weaker national structures or concentrate their resources on their main objectives. More states will be unaffected by mass attacks and will be able to develop essential internal and collective regional resilience to the surprise attack that the sheer complexity of cyberspace inevitably allows.[64] The more unaffected states there are who are also allies, the more likely these unaffected states will have the resources to offer mutual support to defending states.

Finally, the United Nations as an international forum negotiates between states whose roles, responsibilities, and territories are established. Its agencies and commissions will provide mechanisms for nations to quietly and practically cooperate even if they publicly are at odds. When cyberspace becomes a more normalized international system for modern states, one might see cyber ambassadors at UN agencies or cyber attachés at embassies to physically and rapidly calm crises or to coordinate responses if cyber systems are under assault.[65] Rules of conflict resolution and acceptable cybered civil society engagement are collectively, not individually, developed and enforced. When states are cybered entities with sovereign boundaries and can represent and defend themselves in the face of cybered conflicts, a relatively

less predatory and chaotic era of cybered states and rule regimes is likely as the globe continues its relentless digitization across all facets of human society.

Conclusion

In the near future, states will delineate the formerly ungoverned or chaotic cybersphere by formal agreement. In the new cyber–Westphalian process, digital regions complete with borders, boundaries, and frontiers that are accepted by all states will inevitably emerge. The rising virtual mirroring of what has been painfully carved out in the concrete world is not all that undesirable for societal stability, economic returns, and international security. Individuals, a wide variety of social organizations, and, certainly, most forms of commerce thrive on order and regularity. In the material world, we know how to handle cross-border wars and attacks in ways that we struggle nearly in vain to handle cross-border embedded, grey threats masked by the density of modern processes. In the cybersphere, borders will emerge internally within nations as well as externally as the usual commercial and personal security bulwarks against free riders and thieves. Once the borders have emerged, police and national laws will hold sway as they do today in the modern nation-state. However, in much the same way as they operate today in the physical world, attacks across borders will become state responsibilities, whether or not the state approves or guides the attacks.

As the process emerges from inklings to the self-evident, the implications of pulling cyberspace back into the known world of international relations are profound. Today a rough consensus is emerging that something about the frontier nature of the web has to be regulated, either by individual states or by enforceable international regimes. But until the last few years and the dramatic success of the Stuxnet attack, the debate was as much about an international regime as it was about a nation-by-nation response. The international regime approach, however, is fraught with time and attribution difficulties. Not only can such a regime take decades to build, enforcing it as the web stands today will require the very thing current topology of the web does not offer—a way to verify the identity of (and therefore sanction) the violator. The result is, wittingly or unwittingly, individual states have started down the path on their own toward controlling the way the web affects their citizens, organizations, and critical elements of the society. The transition, of course, still lies ahead. SSQ

Notes

1. *Cybered conflict* differs from *cyber war* or *cyber battle*. The latter is fully technological and could, in principle, be conducted entirely within a network. It is normally a component of the former. A cybered conflict is any conflict of national significance in which key events determining the path to the generally accepted outcome of the conflict could not have proceeded unless cyber means were nonsubstitutable and critically involved. The terms are distinctively and deliberately used in this article.

2. Nicolas Falliere, Liam O. Murchu, and Eric Chien, 2010. "W32.Stuxnet Dossier: version 1.3," http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

3. Susan W. Brenner, "Distributed Security: Moving Away from Reactive Law Enforcement," *International Journal of Communications Law & Policy* 9 (December 2004).

4. For example, as the critical infrastructure of Westernized nations such as the United States 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, OR. Had the thief wanted to harm the citizens, taking over the computer remotely to disrupt or destroy the water filtration system would have been exceptionally easy. Even the apparently mistaken theft could have been worse had the thief simply used the machine in situ to ruin the filtration system or poison it. "Theft In Molalla [Oregon] Reported To Department Of Homeland Security: Computer Controlled Town's Water System," *KPTV.com Homepage: Portland News*, 26 March 2010.

5. Isaac Porche, "Stuxnet is the world's problem," *Bulletin of the Atomic Scientists*, 9 December 2010.

6. David E. Sanger, "Iran Fights Strong Virus Attacking Computers," *New York Times*, 25 September 2010.

7. J. B. Michael et al., "Integrating Legal and Policy Factors in Cyberpreparedness," *Computer* 43, no. 4 (2010): 90–92.

8. Threats are considered so serious that cyber-security officials are now expected to have training in known hacker methods. Bill Gertz, "Inside the Ring: Hacker Training," *Washington Post*, 4 March 2010.

9. Nigel Kendall, "Global cyber attacks on the rise: 75 percent of companies have suffered a cyber attack, at an average cost of $2 million, says Symantec security survey," *Times* (London), 22 February 2010.

10. Gillian Wong, "Chinese police shut down hacker training business," *Washington Post*, 8 February 2010.

11. The history of the American railroad, for example, included reaching out to the towns along its path to control the uncertainties that independent but gouging store owners imposed on the passing freight lines and passengers. Renate Mayntz, "The Changing Governance of Large Technical Infrastructure Systems (LTS)," in *Conference Paper: Complexity and Large Technical Systems*, Meersburg, Germany, 2008.

12. Given human history, it does not much matter what precisely initiates the conflict; rather, it is the dependence of one or both parties on a pass, waterway, or global underlying socio-technical system that determines the targeting on those items. Nomads had no fixed address, but they certainly had a sense of their rights to seasonal food crops and were willing to fight to exclude other groups to assure their own survival. R. L. O'Connell, *Of Arms and Men: A History of War, Weapons, and Aggression* (London: Oxford University Press, 1989). See also Charles Tilly, *Coercion, Capital, and European States, AD 990–1992* (Malden, MA: Blackwell Publishers, 1992).

13. Stephen Krasner, "Shared Sovereignity: New Institutions for Collapsed and Failing Status," *International Security* 29, no. 2 (Fall 2004): 85–120.

14. Charles Tilly, "Cities and States in Europe, 1000–1800," *Theory and Society* 18, no. 5 (1989): 563–84.

15. Rajesh Tandon and Ranjita Mohanty, "Civil Society and Governance: A Research Study in India," in *Global Comparative Research Study on Civil Society and Governance* (Sussex, UK: Society for Participatory Research in Asia, 2000).

16. Joseph S. Nye Jr., "Cyber Power," Harvard Kennedy School, 2010, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

17. Duncan B. Douglass, "An examination of the fraud liability shift in consumer card-based payment systems," *Economic Perspectives* 33, no. 1 (1st qtr., 2009): 43–49.

18. Ross Anderson et al., "Security Economics and European Policy," in *Managing Information Risk and the Economics of Security*, ed. Eric Johnson (New York: Springer, 2009), 55–80, http://weis2008.econinfosec.org/papers/MooreSecurity.pdf.

19. D. Lindsay, "Liability of ISPs for end-user copyright infringements," *Telecommunications Journal of Australia* 60, no. 2 (2010).

20. Michael Evans and Giles Whittell, "Cyberwar declared as China hunts for the West's intelligence secrets," *Times* (London), 8 March 2010.

21. Elinor Mills, "Web traffic redirected to China in mystery mix-up," *CNET*, 25 March 2010.

22. This effect, according to John Mallery, is a national cyber security means of increasing the "work factor" of the bad actor. The key strategic goal of cyber defense is to raise the work factors for attackers and to lower them for defenders. Work factors are conceptualized along dimensions of computational complexity, cost, cognitive difficulty, risk and uncertainty, cultural factors, and information differentials. See John C. Mallery, "Towards a Strategy for Cyber Defense," presentation at the US Naval War College, Newport, RI, 17 September 2010.

23. Douglas M. Gibler, "Bordering On Peace: Democracy, Territorial Issues, and Conflict," *International Studies Quarterly* 51, no. 3 (September 2007): 509–32.

24. Narushige Shiode, "Toward the Construction of Cyber Cities with the Application of Unique Characteristics of Cyberspace," *Online Planning Journal*, 1997, http://www.casa.ucl.ac.uk/planning/articles21/urban.htm.

25. On this point of curbing outward attacks, a functioning government controls the means of violence within its nation and that would include the means of enabling one of its citizens to attack another nation without governmental approval.

26. Kathrin Hille, "How China polices the Internet," *Financial Times* online, 17 July 2009.

27. Joel F. Brenner, "Why Isn't Cyberspace More Secure?" *Communications of the ACM* 53, no. 11 (November 2010): 2.

28. Paul Cornish, Rex Hughes, and David Livingstone, *Cyberspace and the National Security of the United Kingdom* (London, UK: Chatham House, 2009).

29. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Washington: RAND, 2009).

30. Pam Benson, "Computer virus Stuxnet a 'game changer,' DHS official tells Senate," *CNN*, 17 November 2010.

31. Michael Wines, Sharon LaFraniere, and Jonathan Ansfield, "China's Censors Tackle and Trip Over the Internet," *New York Times*, 8 April 2010.

32. Ching Cheong, "Fighting the Digital War with the Great Firewall (op-ed), *Straits Times*, 5 April 2010.

33. Three of the world's largest sites are banding together with two of the largest content distribution networks, Akamai and Limelight, coordinated by the Internet Society, to declare 8 June 2011 World IPv6 (Internet Protocol version 6) Day. "Google, Facebook and Yahoo Partner

for World IPv6 Day," *Softpedia.com*, 12 January 2011, http://news.softpedia.com/news/Google-Facebook-and-Yahoo-Partner-for-World-IPv6-Day-177852.shtml.

34. Ben Worthen, "Internet Strategy: China's Next Generation Internet," *CIO.com*, 15 July 2006, http://www.cio.com/article/22985/Internet_Strategy_China_s_Next_Generation_Internet_ .

35. Rebecca MacKinnon, "Commentary: Are China's demands for Internet 'self-discipline' spreading to the West?" *McClatchy Report: Washington Bureau*, 18 January 2010, http://www.mcclatchydc.com/2010/01/18/82469/commentary-are-chinas-demands.html.

36. Mike Masnick, "The Similarity Between ACTA and Chinese Internet Censorship," *TechDirt* online, 20 January 2010, http://www.techdirt.com/articles/20100120/0216537828.shtml.

37. "China keeping closer eye on phone text messages," *New York Times* Technology Section, 6 December 2005.

38. Sharon LaFraniere, "China to Scan Text Messages to Spot 'Unhealthy Content'," *New York Times*, 20 January 2010.

39. Wines et al., "China's Censors Tackle and Trip Over the Internet."

40. Lucian Constantin, "Attack Hits Swedish Signals Intelligence Agency's Website," *Softpedia News*, 6 November 2009.

41. Evans and Whittell, "Cyberwar declared as China hunts for the West's intelligence secrets."

42. Anthony Lloyd, "Britain applies military thinking to the growing spectre of cyberwar," *Times* (London), 8 March 2010.

43. Lance Whitney, "U.S. Cyber Command prepped to launch," *CNET News—Security*, 23 March 2010.

44. William J. Lynn, "Defending A New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010).

45. Emily Goldman and Leslie Eliason, *The Diffusion of Military Technology and Ideas* (Stanford, CA: Stanford University Press, 2003).

46. Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law* 25, no. 3 (May/June 2009).

47. "South Korea to set up cyber command against North Korea—two years earlier than planned," *Channel News Asia* online, 9 July 2009.

48. Richard J. Aldrich, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: HarperCollins, 2010).

49. Ellen Nakashima, "Pentagon's Cyber Command seeks authority to expand its battlefield," *Washington Post*, 6 November 2010.

50. US laws enable "authorities" to draw legislative lines between offense (a military "Title 10" authority), defense (of military, "Title 18"; or of the wider government, a DHS mission), and the collection of national intelligence (a "Title 50" mission given the National Security Agency as primus inter pares electronic collector among other intelligence agencies).

51. This structural compromise was unusual for the United States, and it was hotly debated in the Congress before the first commander, Gen Keith B. Alexander, was confirmed as head of both agencies. Winning the debate were the need for a very wide intelligence view, a high level of skills, and the military ability to move quickly, as well as the character and expertise of the new commander himself. Ellen Nakashima, "Gen. Keith Alexander confirmed to head cyber-command," *Washington Post* online, 11 May 2010.

52. Even the loss of laptops, treated casually just years before, now engenders enormous legislative concern and recriminations against agencies even indirectly responsible for the cyber security of the nation as a whole, such as the GCHQ intelligence agency. " 'Cavalier' GCHQ online spy centre loses 35 laptops—Centre also struggling to keep up with national cyber threats," *Computerworld UK* online, 12 March 2010.

53. Richard Norton-Taylor, "The UK is under threat of cyber attack," *Guardian* online, 18 October 2010.

54. See the website http://www.ssi.gouv.fr/site_rubrique97.html, hosted by ANSSI, which rather openly discusses its successes in strengthening cyber defenses.

55. "EU and US join NATO cyber security pact," *Computerworld UK* online, 10 November 2010.

56. Cheryl Pellerin, "DOD, DHS Join Forces to Promote Cybersecurity." *American Forces Press Service*, 13 October 2010.

57. Private conversation with senior civilian cyber-security police official in Germany, October 2010.

58. Even the Chinese government has felt the need to have a cyber command equivalent and publicly announced its creation of a cyber warfare unit as a defensive measure in response to the provocative actions of the US government in creating a cyber command. Tania Branigan, "Chinese army to target cyber war threat," *Guardian* online, 22 July 2010.

59. "European Union Considers Stronger Cybersecurity, Stricter Penalties for Hackers," *New New Internet* (*TNNI*) online, 1 October 2010.

60. John Markoff, David E. Sanger, and Thom Shanker, "Cyberwar: In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times*, 26 January 2010.

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

62. Gene I. Rochlin, *Trapped in the Net: The Unanticipated Consequences of Computerization* (Princeton: Princeton University Press, 1997).

63. Tom Espiner, "UK launches dedicated cybersecurity agency," *ZDNet UK* online, 25 June 2009.

64. The process of moving to better internal resilience is elaborated in a forthcoming book. The work argues for and outlines a security resilience strategy involving both disruption and resilience via cybered institutional capacities developed and adapted at the national level. Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens: University of Georgia Press, 2011).

65. Jaikumar Vijayan, "After Google-China dust-up, cyberwar emerges as a threat: The episode highlighted cyberthreats facing the U.S., but it's not a war—yet," *Computerworld*, 7 April 2010, http://www.computerworld.com/s/article/9174558/After_Google_China_dust_up_cyberwar_emerges_as_a_threat.