CHAPTER 8

Cybered Conflict, Cyber Power, and Security Resilience as Strategy

Chris Demchak

National Surprise from a Densely Populated Cybered World

THE UBIQUITY, CONNECTIVITY, AND CRITICALITY of cyberspace changes national security balances throughout the globe. Cyber power transcends geography's natural barriers and can cause harm to others on varying scales while the cyber actors remain safely a long distance away.[1] Among the concepts requiring adjustment for this emergent age are cyber war, cyber power, and the appropriate reach of effective national security strategy. This chapter makes two arguments. First, "cybered conflict" is a better term than "cyberwar" for the kinds of national-level struggles endemic to the interdependent complexity and scale of the world rising up around us.[2] The term helps frame the complexity of conflict involving cyberspace, especially for those making decisions about how to develop a strategic response to threats. Actions meant to harm another nation will not stay contained within legacy military notions of a battlefield "domain" or even within the networks that enable global attacks.

Second, national cyber power and its associated strategy for national security must include internal societal preparations for surprise as much as external disruptive projections to avert offensive cyber asymmetries. The new normalcy of cybered conflict is its enduring potential for cascading unexpected outcomes anywhere across the deeply interconnected and complex critical systems of a modern society. A national security resilience strategy offers the necessary composite framework to guide and explicitly coordinate society's cyber resilience with the national military capabilities developed to secure national borders. Recognition of this new composite form of national power and the corresponding security resilience strategy is emerging indirectly across the policies and institutions of westernized nations, but these are early days yet.

Cybered Conflict, not Cyber Domain or War

For an emerging variety of human conflict across a densely connected digital globe, "cyberwar" is too narrow a term.[3] In the emerging cybered age, cyberspace is a ubiquitous substrate, not merely one domain among many others. Any conflict of concern to a nation-state is likely to develop far beyond the purely electronic hostilities occurring entirely within electronic networks of a "cyberwar."[4] Rather, "cybered conflict" better captures the ambiguities and extends the national security dilemma today. A cybered system is more than its cyber underpinning; it includes all sorts of systems of people, things, processes, and perceptions that are computer-related but not necessarily purely computerized.[5] Phishing can be an attack even if it simply sends information to bad actors through the foolishness of the email recipient.[6] The purely cyber portion could constitute a preparatory phase, a main avenue of attack, a central campaign element, a large-scale deception and espionage operation, an episodic enabler, a foregone set of activities, or all of these at different times in a long-term cybered conflict.[7] The entire conflict, however, is cybered if the exchanges of weapons and damage do not stay within the networks but rather seep or explode beyond the technical into the wider organization or society.

In fall of 2010 the broader, inclusive cybered conflict emerged explicitly in the international system. With the damaging attack on critical Iranian nuclear reactors, a malicious piece of software called Stuxnet became the first publicly known cyber weapon to cross over from the bytes of electronic networks into direct physical sabotage of large-scale industrial systems. Its success heralded the arrival of the era of cybered conflict. This particular malicious worm struck Iran's nascent and internationally contested nuclear reactors in situ in Iran far from any foreign military installation. Even though the reactors were disconnected from the internet, the software directly disrupted the process of moving the reactors into full operations.[8] Unlike other viruses and malware, Stuxnet matters globally because it showed the path of preference for future attackers on all sides in the emerging era. From here on, every fight will be cybered at key points before, during, and after the main effects.[9]

The Stuxnet designers demonstrated to the rest of the world how the attack advantages of a globally unfettered, easily accessed, and readily used cyberspace can be employed against enemies. Over the course of about two years, the Stuxnet application on innocent USB mobile drives copied itself often and spread far enough to end up where the iterative designers wanted—inside a large-scale technical plant not connected to the internet. If it traveled to an internetted machine, the code opened a backdoor to two URLs and requested an update. For those infected systems without an internet connection, the program had to be able to deliver its final payload without an update. As a result, the payload was buried in code that also hid its activities from the operator. While the operator stared at a screen whose code said the machine tests were within expectations, the actual commands changed by Stuxnet ordered the centrifuges to oscillate wildly with no human in the loop. Ultimately, despite Stuxnet having wandered into thousands of other systems in India and

China, for example, the damaging payload was delivered as planned and the Iranian nuclear reprocessing program was delayed for at least one to two years.[10]

Stuxnet also showed how state-level conflict and criminality are and will be intricately linked in the cybered conflict age. The bundled modules harnessed the delivery and stealth skills of exquisitely good cybercriminals to the intents and probably state-sized funding of cybered warriors to produce a physical effect. In the Stuxnet case, there was no downside for the attackers in borrowing the cybercriminal's delivery methods or types of covert infection codes. Furthermore, intelligence was automatically acquired as the Stuxnet worm wandered around, checking for updates from two key URLs if an internet connection was available. Not only did these callbacks tell the owners of the URLs where Stuxnet had landed, they also provided critical operational system data about every other nontargeted system the worm passed through in its search for its target. Until the two websites were closed down in summer 2010, the designers of this cyber weapon obtained a great deal of information about thousands of infected systems that could prove useful in later conflict operations or even business competitions.

Stuxnet did not need to be connected to the internet to cause the intended damage. This "fire and forget" aspect of a cyber attack represents the increasing levels of ongoing threatening surprises inherent in future cybered conflict. For the future, it will not be wise to assume the odd bit of seemingly innocuous code that has floated into one's computer system from all directions is safe because it has no obvious effects or infection pattern.[11] What may have seemed safe in the neighbor's systems might find in one's own computer its specific target, the computer DNA the small bit of software targeted for harm. The benign lost code might suddenly then issue its disable, disrupt, deceive, or destroy command.[12] The innocence of the utopian cyber prophets from the 1990s is now firmly gone.[13] The same people who orchestrated this industrial level of sophisticated application development are today still out there, able to do it again, for whatever reason or for whichever employer. Variations of the Stuxnet worm are in the wilds of the hacker international world now. It is almost certainly the target of reverse engineering all over the world by thousands of computer hackers, government scientists, cyber warriors, or commercial consultants. "Son of Stuxnet" is inevitable as an employed tool, along with its cousin or distantly related code attempting to replicate the demonstration event of the original.

While it is now relatively easy to find a Stuxnet infection, its children and lookalikes will not be so easy to locate. The follow-on worms are likely to be repurposed for any number of targets and delivery systems. Stuxnet floated around for at least a year before even being noticed and largely ignored by the major antivirus firms. It is easy to imagine a campaign of many Stuxnet-like variations released all over the world in a sort of "tailored DNA swarm" that floats for some time without apparent effects. Today this kind of assault can begin with all sorts of actors and reasons, challenging societies across all sorts of connections that reach deeply into their internally critical spaces.[14]

What is emerging is not the traditional environment of war for which most modern militaries prepare. Cyberspace does not fit into the framework of a military "domain," a term used by the US military in particular to blend cybered conflict into the traditional molds of competitive armed struggles. As a global, synthetic substrate, cyberspace is an arena, tool, weapon, and enabler of conflict with implications in threat and harm beyond the normal military four fields of battle: land, air, sea, and space.[15] In 2009 the US military officially declared cyberspace a military domain, immediately spawning a large number of repetitive conferences trying to fit cyberspace into concepts derived from existing air, land, sea, and space domains.[16] The domain designation may be useful for parsing the lines of authority among military services, at least bureaucratically, and it also may make for more accustomed objectives if a national military seeks to dominate the enemies in the cyber domain. Cyberspace is not, however, a conveniently bounded fifth domain offering some kind of limit of action, knowledge, operational effect, or even conflict.

Nor does cyberspace demonstrate attributes equivalent to those of the nuclear domain in weapons, deterrence, or systems. Nuclear weapons are highly specialized and centrally developed. As topics of deterrence, the technology is the central point of intensely debated international regimes and its proliferation both reviled and inhibited. As systems, they are remarkable in their (fortunate) lack of use. The cybered substrate is dual-use, wantonly proliferated without identification of locations or owners, and used continuously. It stretches ubiquitously into, across, and throughout the society that the military is trying to protect as well as outward to the world from which the attackers may come. No identified domain of war offers the equivalent scale and complexity of cyberspace as a globally shared system that consistently intrudes into, connects at long range, and induces behaviors transcending traditional boundaries of land, sea, air, institution, nation, and social or technical medium.[17] In the same way the term "cyberwar" fails to capture the true complexity of the challenge, the designation of a cyber "domain" does not help guide any national leader in dealing with the cybered conflict age.

From here forward in the digitally connected globe, conflict will be cybered. Cyber networks will always be involved state-level conflicts, whether with another state, nonstate actor, or both, but conflict of national significance will not stay purely within the networks. The cybered age has been built up under the collective feet of westernized societies focused on ecommerce and communication without borders. In the cybered world, humans in their own groups have engaged in a process well known in ecological systems studies as *autopoiesis*. Like ants dumping their debris out their front door and creating ant hills they then have to climb up and down, modern societies collectively built the big security obstacles to which each society now must individually adapt.[18] Conflict will travel along any path of human or machine exchange enabled by cyberspace.

In the modern world, one cannot leave cyberspace and go home.[19] Cyberspace never evolved into a sort of information-enabled Eden filled with nice, sharing people who recognized and ethically supported the desire of information to "be free."[20] Rather, a good analogy may be that cyberspace is a globally unfettered exchange

space more like an enormous, muddy, colorful, moderately chaotic, annual medieval fair without adequate security from an overlord or the town leaders and with all the human energy and pathologies possible in shared space.[21] One can even associate archetypes. While offering great and new resources, the fair exchange stalls and spaces (cyberspace's e-commerce and social websites) were also replete with conniving paupers (script kiddies), pickpockets (small-time credit card thieves), con artists (phishers, social engineers, ID thieves), and organized competing gangs of muggers (huge professional botnet masters), along with occasional wholesale attacks by armed brigands (organized cyber gangs, national-level covert cyber units).[22] Occasionally overwhelming force by an opposing or angry aristocrat would crush the entire event physically, if necessary.[23] In short, while the fair was always an economically energizing place, it was never safe. Always present was a good chance of dangerous surprises for individuals and less powerful groups set upon by others known or unknown to be enemies in advance. Cyberspace goes much further than the medieval fair in its continuousness, more like the medieval age in its ubiquity, and its corollary cybered conflict flows into the same places as cyberspace. A globe's volume of human pathologies can operate all the time using cyber means to reach and harm others anywhere, through any mode of access into the internet, and for whatever enduring or spontaneous purpose.

Put more formally, cybered conflict is distinguishable from cyberwar by the course and national significance of effects beyond the functions of the network. A cybered conflict is any conflict of national significance where success or defeat critically depends on cyber means in key activities over the course of all relevant events. A purely cyber conflict or war, in contrast, stays largely within the technical networks of cyberspace. Combatants of all levels and numbers gain access, steal data, and leave destroyed but quickly replaceable computer hard drives behind. Beyond the networks, little else happens in the wider society that is clearly disabling either widely or for long. The hard drives are replaced, backed-up data is reloaded, and a new round of spy/criminal-versus-malicious-spy/criminal begins. Cybered conflict may not involve any direct harm to any machine on any network. The major thrust of the attackers' operations could be quite covert and yet could leak outside the networks with serious effects. A major attack campaign could rest on a small set of independently spread, singularly covert pieces of software, each of which ultimately spreads across a limited or large number of critical nodes in a key system and changes their functioning in nonobvious ways. The resulting inaccurate operations could continue over long periods without recognition, especially if the changes across several critical values in internal but basic transactions vary erratically enough and the harm seems more a high level of normal accidents. Yet, in the process and over time, crucial decisions across the wider societal institutions could be misdirected, enfeebling defenders and the wider society.

Owing to its emergence in and through a global cyberspace, cybered conflict has distinctive characteristics that include universality and high tempo in participation across widely dispersed populations, ubiquity in intrinsic surprise potential across sectors and levels of society, and indeterminateness in its duration. First, its volume

of attack tempo is high due to the massive number of potential bad actors anywhere in the globe who, with limited skill, can easily access and abuse the openness of the internet.[24] Any individual can for any reason use scale, proximity, and precision advantages formerly only open to either close neighbors or super powers. That is, all along the passageways of cyberspace, individuals can organize an attack organization at a scale from five to five thousand co-combatants. The same bad actor operating on the internet can plan to attack from a safe location ranging from five miles to five thousand miles within proximity of the targets. Finally, that actor, group, or state and fellow travelers can select with standardized cyber weapons and an unprecedented range of precision any set of targets from one state, group, or individual to combinations of whole regions, communities, or societies. Normal barriers to entry to this kind of pathological behavior do not operate in the current topology of cyberspace, making very small the likelihood of being able to stop bad actors or their attacks before the operations are launched.

Second, cybered conflict will always involve a large number and wide range of surprises across integrated networks. Either these will be foreseeable (in form or frequency) or rogue (unforeseeable) surprises, but they will always be present due to the intrinsic complexity of the streaming and converging globally cybered systems and the attack advantages given to bad actors anywhere around the globe today. Unexpected nasty events will come by accident, by intention, by opportunism, or all three simultaneously. Outcomes will embody the full variety of what complex systems, including people, can perpetrate on one another at a distance, thus ensuring the safety of attackers. For example, hurricanes can destroy electrical grids, and so might hackers. Hurricanes, however, will not change their strategies in order to make the damage and suffering even more debilitating when the responders show an ability to recover quickly. Moreover, others not involved as central parties to a conflict will often enough use the cyber substrate to act maliciously as well, to "pile on" in others' conflicts without much risk or even a clear objective. A world in which global climate change is making climate turbulent and more dangerous now offers a global passageway by which others could conceivably reach inside a nation responding to a natural disaster and worsen the cascading harm for whatever reasons that may motivate their decision to act.

Cybered conflict thus presents a new form of normalcy in its imposition on national systems of this increased potential for nasty surprise across a society. Nationally critical systems can no longer depend on obscurity or the goodness of strangers in order to be left alone to operate safely. Such a level of uncertainty is unprecedented in its near ubiquity across all levels of society, but it is far from historically unknown. Facing daily insecurity has been a well-known situation for most individuals throughout history. For pioneers in the 1860s in the United States, for example, nothing one needed could be presumed to be safe. From the safety of the dried food, to drinking water, to the companions on the trail, to the path through the wilderness that a scout directed—all could deceptively look robust and yet fail at any moment, and do so critically. What the spread of the cybered world has done is

reintroduce modern societies by their own actions to a much older "frontier" level of insecurities.[26]

Third, cybered conflicts are uncomfortably indeterminate in how the participants' struggles for control of outcomes begin, endure, or end—if ever they ever do. Many conflicts will begin with no particular warning and no clear indicators of how long, far, or deeply this particular struggle might progress. With global scale, at any given moment some actors somewhere will be trying to change the allocation of—or access to—physical, reputational, or even projected resources in ways they desire and for rationales they may alone accept. With ubiquitous access to the global cyber passages, a vast number of actors at any given moment will employ any cyber means available to them at costs and risk levels they can accept in pursuit of the outcomes they seek. There are currently no natural barriers to entry in this bubbling competitive struggle for preferred outcomes. The flood of attacks can come from anywhere for literally any reason and can last as long as the rationale, the means, or the lack of personal risk exists. At any given time, thousands of such actors are operating through cyberspace precisely because it is so easy, useful, and accessible without the local societal constraints developed over centuries by modern societies.

As a result of these attributes the combinatorial possibilities of cybered conflict are exceptionally difficult to accommodate, making the current focus of more democratic national strategies on the technical aspects of cyber attacks misplaced and even dangerous. The concept of a cybered conflict is necessary to move national security focus to a more integrated system approach consistent with the challenges cyberspace actually imposes. The enormous scale of material traveling through cyberspace is such that small campaigns with swarms of such small changes, perhaps inserted by hijacked updates, can be routinely conducted unnoticed as a whole, each time adding a bit more to the troubling variability threatening wider critical national systems. The effect could be to continually sow distrust, inefficiencies, losses, and harm to a society, perhaps in conjunction with a planned military action or perhaps merely to attrite the defending nation's economic strength over time so as to make the planned action much easier to persuasively pursue. Far from the networked nodes affected, national leaders could make inaccurate or ineffective decisions based on distorted guidance about the reliability of the nation's GPS system or electrical supply, or the integrity of data driving targeting in military operations, or massive capital flows in national financial calculations. They could focus on the cyber aspect of the conflict but miss the wider ripple effects of the cybered struggle and its effects beyond a cyberwar in breadth, extent, and significance.[27] Beyond the term's conceptual advantage in understanding what is changing for security in a cybered world, using the term "cybered conflict" allows both technical and nontechnical experts to sit at the same table to collectively design national policies for cybersecurity. The more comprehensive "cybered" adjective moves the national security debate beyond defending networks or attacking back through them. Policymakers are better able to jointly see the emerging security dilemmas of large-scale complex societal-technical systems across the entirety of a modern nation.

The adjustment in concepts is critical across a wider range of concepts and terms of art in order to make them more congruent with the emerging world. With the "cybered" characterization, the cybered conflict aspects of other well-known forms of struggle such as hybrid warfare, asymmetric conflicts, and counterterrorism campaigns are easier to integrate with the cybered age. Even in these forms of struggle and defense operations, key events will depend on the cyberspace substrate for completion.[28] Furthermore, the internationally accepted rules of war are now under debate, appearing to have trouble in application to cyberwar. With a broader, more systemic notion of conflict as cybered, these rules would find more resonance with much of what happens to the overall system before and during a struggle that has not quite broken out into kinetic exchanges.[29] Even experts in the history of traditional war and those in the development of social media networks could avoid having endless debates in their own communities about whether cybered conflict is or is not relevant to their area of expertise.[30] The systemic nature of threats forces each community to link to other areas of expertise to address the ubiquity of cyberspace. its complexity in reach and unprecedented intrusions, and its unpredictably tough dual-use nature. In the developing age of cybered conflict, national power depends on how all the skills sets work together against nasty surprises that travel far beyond the underlying cyber networks.[31]

Cyber Power and a National Security Resilience Strategy

In a deeply cybered world, notions of national power and the content of national security strategies need to change if the well-being of the nation is to be maintained. Cyberspace as a globally unfettered system alters the relative distribution of international influence available for state or nonstate actors. National cyber power will have to address global complexity directly throughout its wider arena of operations and threat assessments. Definitions and institutionalized implementation of national power will perforce begin to reflect a more systemic, less traditional war-related framework if one is to face successfully the wide variety of surprising threats that could emerge from widely connected, asymmetric actors.[32]

In particular, the dual-use nature and ubiquitous reach of cyberspace push a nation's national security concerns to widen and to be more inclusive in order to effectively anticipate and respond when the society is surprised. In the emerging cybered age, cyber power for a nation will always rest on the nation's coordinated abilities both to disrupt likely and ongoing incoming cybered surprises and to be resilient through systemic internal preparations against the inevitability of successful attacks. When the attacker can use the cyberspace substrate in unprecedented, novel ways, society's security will depend on its already well-embedded abilities to hit and heal in ways commensurate with the significance of potential harm.

Cyber power today is defined as the ability of a nation's leaders and institutions facing cybered conflict to keep the overall uncertainty across nationally cybered systems down at levels tolerable for their citizens' expectations of normal well-being. In

practice, dissipating disabling threats internally means creating national "breathing space" against the harm planned by remote cyber bad actors or the damage emerging in current attacks that have already gotten inside the nation's systems. Cyber power based on a dual-robustness in responses to impede in advance or endure in response will be tailored over time in the relative emphasis given each component according to the circumstances of vulnerability of the nation at risk. Nonstate actors could conceivably have as much cyber skill as the defending state actors, or more. A rather common outcome of a narrow focus on cyberwar is developing cyber-attack means without commensurately developing the resilience of systems that attackers will target in the wider society. Effective national power will depend on the ways in which internal and external national actions and abilities in cyberspace are balanced and sustained over time and experience.

One indicator of a nation's cyber power is the effective reduction of the advantages that cyberspace affords attackers even if they do not solely use cyber means to cause harm.[33] In some cases, attackers may only be able to organize a sufficiently large number of fellow actors or infected computers as long as they are insulated from discovery by local police or even from networked retaliating defenders.[34] In other cases, the attackers may be able to persuade opportunistic fellow travelers to pile on in such numbers that personal identification becomes irrelevant. In these circumstances, negating the effects by being internally quite resilient dampens the enthusiasm to keep up the attacks across large numbers of loosely affiliated bad actors. If one cannot find or reach the attackers, a state with a great deal of cyber power can frustrate them with additional emphasis on resilience, producing the same effect as having individually silenced each attacker. The nation sustaining the dual aspects of cyber power continually disrupts efforts at attack where possible but always ensures that it survives well through any attack successes.[35]

National security strategies designed for a cybered age must develop this dual set of capabilities for effective cyber power. A security resilience strategy combines both traditional notions of security with nontraditional notions of resilience. No longer can a nation have its security agencies only look outward to possible enemies and avenues of response when, using the access and three attack advantages of cyberspace, attackers can bypass military forces and physical borders completely. Unlike the terrorists of al-Qaeda, the cybered conflict attackers do not have to physically enter the targeted nation, group, or community. The emerging densely populated, unequally resourced international system poses composite security challenges inside nations, requiring national security organizations to have key multilevel roles that they have not had since before the Cold War.

First, in a complex social system under threat, national-level agencies will have to engage in coordinating and guiding redundancy, slack, and continuous trial-and-error learning across critical internal national systems as much as identifying specific hostile foreign actors and attacking or negotiating with them across national borders. These policy challenges of cybered conflict might well be captured with two critical adages for the security strategist at any organizational scale: beware and prepare. The national security strategy must orchestrate the natural tendencies of its

society to do both to meet surprise in its critical systems. If organizations are digitally and globally connected to each other to obtain something critical to their respective ability to operate, then one cannot sensibly fully trust anything reachable from those connections, or any aspect of the larger systems to which they link. National security rests on a shared public-private organizational recognition of the deep penetration of cyberspace's global scale and complexity into all critical societal systems. As easily as the great benefits of economic efficiencies and knowledge exchanges come throughout the internet, likewise come all the traditional forms of human greed, pathologies, and cruelty—only more subtle and persistent.[36] The national security strategy needs to encourage instinctive and dedicated wariness. Cyberspace is the same old medieval fair, but it now includes mercenaries, lords, scalpers, and grouped predators that come from near and far, and can all operate on the same set of targets simultaneously and suddenly. For the same level of security of thirty years ago, the national security policy must be able to interdict the worst aspects of this behavior at greater distance, higher levels of unexpectedness, and fantastically accelerated speed in a cybered globe.

Second, national policies must prepare its home society for the reality, however infrequent but inevitable, that their critical systems will fail at some point. The origins may be accidental or deliberately instigated, but the nation's responses must expect that the harm can be exploited, extended, or exacerbated by attentive attackers operating safely immune across open cyber passageways from somewhere around the globe. For example, in early 2011 Libyan rebels fighting the forces of the dictator Muammar Gaddafi found that the social media sites they were using to organize operations were under intense disabling cyber attacks by Serbian ultraconservative groups far from North Africa. The Serbian groups' rationale for this "pile-on" was that they hated NATO for helping Kosovar rebels in 1999, and attacking the Libyans was a way to make things hard for NATO. They were not materially involved in the Libyan struggle, nor did they care about the consequences for the Libyans themselves. Rather, in a demonstration of the variety of likely combatants in any future cybered conflict, the Serbians joined in simply because they could express their grievances using the attack advantages of cyberspace.[37] National security policies need to develop the national understanding that organizations and individuals so deeply connected must practice in advance to operate without the benefits or the machines involved with possibly little or no notice.[38]

For post-Cold War modern democracies, having a national security policy address domestic security issues is normatively, institutionally, and legally troubling, but the circumstances of the unbounded cybered world require it for strategic well-being. The complexity and scale of cyberspace do not stop at national borders today. Securing complex interdependent and critical systems requires extraordinary knowledge about large-scale societal systems at home as well as all those between the defending nation's outer limits and likely sources of any attack.[39] Before the Cold War era, military writers (outside of nations with large strategic buffers such as oceans) recognized that wars on one's home soil inherently blended two external and internal imperatives—externally repel and internally endure. War of existential consequence

was always going to be total, if for at least one state-level combatant. Every nation needed to have forces and policies to deflect attackers from national territory and to be prepared to withstand the attacks inside the borders. Indeed, historically, such a level of internal as well as external insecurity usually meant that military forces operated both inside and at the border. Police forces did not emerge until later in the development of the modern state, when enemies as the main source of societal insecurities could reliably be pushed physically outside recognized limits to national territories.[40] Police forces are more efficient forces when the society is largely socialized into accepting the societal control regimes. However, when internal insecurity rose to require coordination across a large number of actors to develop resilience against large-scale disabling surprise, usually in times of war, then history suggests national security institutions were more often the mechanism by which the nation balanced its outward-looking security and its inward-looking resilience capabilities for survival.[41]

During the Cold War era, however, the stable westernized nations disconnected national security cognitively and institutionally from internal resilience largely because recovery in the face of a nuclear war seemed both undoable and unthinkable. What the total war needs of World War II had pushed together, the Cold War consensus between superpowers about staying away from mutual nuclear destruction separated profoundly. Especially in the United States, national security grew to focus uniquely on significant aggressive actors acting from areas outside one's border.[42] Conversely, the concepts of resilience (viewed more as robustness) became the province of strictly domestic national disaster and emergency institutions.[43] Its central concepts and policies were associated with protecting large interdependent societal systems in the face of engulfing environmentally natural surprises. Active enemies have not been included among the possible instigators of a natural disaster, and hurricanes are not seen as national security threats. Therefore, military involvement in natural disaster responses has been routinely relegated to enhancing the normal abilities of domestic services and providing backup capabilities to be used only if the local or domestic authorities are overwhelmed. Bad actors in the geographically bordered world have had to pass borders to cause significant internal harm; therefore, internal security has been left to domestic police forces and external security kept strictly to the military and foreign office domains.[44]

Over the past ten years the external threats to internal systems posed by terrorism and transnational criminal organizations have challenged this artificial domestic versus national security cognitive, legal, and institutional barrier. In the early 2000s key terrorist leaders made explicit declarations of war on whole societies, not just their military or overseas representatives.[45] Threats from cyberspace similarly reach directly into societies. Nonetheless, it has been difficult to overcome the deeply embedded presumptions that external threats should be met by entirely different concepts, strategies, and institutions from those dealing with internal threats to critical national systems. American security studies literature in the United States over the past twenty years shows exceptionally limited use of the term "robustness," or its equivalent. Even today, senior scholars in international relations have been

publicly unconvinced of the national security threat from cybered attack, referring to the possibilities of disabling cyber attacks on a westernized nation as "hyperbole" or "threat inflation."[46] The national security versus domestic safety distinction continues formally today the area of cybered conflict, with internal resilience and responses to international cyber crime dissociated from national security concerns of signatory nations. As long as this distinction holds, the integration of crime with conflict will continue to pose exceptional surprises to nations inside their traditional borders. The global "university of cybercrime" routinely innovates techniques appropriated for effective use by state and nonstate actors who then use the massive noise of cyber criminal operations as cover for their more malicious operations.[47] National strategies for survival and well-being in a ubiquitously cybered world will only be effective when security and resilience concerns blend strategically at the national level. The gap is precisely what enables the harm to enter national systems from the globe's bad actors at every level from criminal to peer state.

Cybered Conflict Age: Rise of Cybered State Borders and National Security-Resilience Strategies

Today the automatic barrier between national and domestic security has thinned; however, more explicit embrace of the possibility of nationwide significant cybered surprise is needed. Given the triple onslaught of transnational criminals, terrorists, and now cyber attackers coming virtually and physically inside traditional national borders from all corners on a global scale, leaders in modern democratic states are moving step by sometimes halting step to develop their nation's ability to repel and endure the harmful surprises of cyberspace.[48] While not explicitly declaring an intent to sieve the walls between the two security policies and communities, key westernized states are iterating toward this recognition in their various expressions of their own cybersecurity strategies.[49] Without using the term in so many words, the recognition of the need to both prevent the attacks and endure the inevitable surprises is present in the US 2009 cyber policy declaration by President Obama, in the 2009 French defense paper that details changes to its national cybersecurity organizations, and in the 2010 British national defense and security strategy.[50] The institutions being established across these nations for the purposes of national cybersecurity vary a good deal, but they begin to demonstrate a nascent recognition of the old-new dual nature of conflict via cyberspacê. Across these and other westernized nations, the new strategies and institutions have begun to show interesting similarities in what critical national functions are to be protected, how actors are to be made aware of threats and responsibilities, and how each national government intends to support security from cybered attacks both internally and externally.[51] For example, while only applying to the US military, the new Department of Defense Strategy for Operating in Cyberspace (DSOC) is about resilience of the forces and even the wider nation.[52] The DSOC requires more clarity, conceptual and institutional development, and the grounding of experience fed back into thinking. However, when the

central arguments of the DSOC are combined with the normative and protective language of the US International Strategy for Cyberspace (ISC), the rudiments of a future explicit national security-resilience strategy guiding national capabilities in both resilience and disruption seem to be present.[53]

A security-resilience strategy will take time to evolve in the format necessary for the circumstances of each nation. Only the United States has formally established a military cyber command, but one may argue that the new authorities and institutions put in place in other nations are likely to act as cyber command equivalents over time. While the United States has emphasized the hit capability over the heal requirements of a security-resilience strategy, France and the United Kindgom have focused on the heal component over the hit abilities. However, both the security and resilience components are critical to national cyber power in the emerging cybered age. In each nation connected to other like-minded groups of nations, eventually some set of balanced institutional mechanisms to achieve national security resilience against cybered conflict will emerge commensurate to the vulnerabilities and likely harm to the nation at risk. Given the advantages of scale, proximity, and precision afforded the attacker today, it is likely that the cyber command as a generic response will be seen in future as the hallmark of a state's willingness to defend its cyber territory as well as endure attacks inside the nation. Similarly, the surprise-embracing aspects of the present across the DSOC and ISC documents are likely to serve to mark the beginning of a wider transformation process in the United States and other westernized states in their efforts to maintain their well-being against the surprises of a heavily integrated, existentially competitive cybered world. The evolutionary twists and turns of national power, strategies, and institutions lie before us. Welcome to the early days of the cybered conflict age.

Notes

Publisher's note: At the request of the author, the term internet is not capitalized.

1. John Markoff, "Cyberwar: Old Trick Threatens the Newest Weapons," *New York Times*, October 27, 2009.

2. Excellent discussions of complexity and its inherent surprises across large-scale systems can be found in the following sources: T. R. LaPorte, *Organized Social Complexity: Challenge to Politics and Policy* (Princeton, NJ: Princeton University Press, 1975); M. R. Lissack, "Complexity: The Science, Its Vocabulary, and Its Relation to Organizations," *Emergence* 1, no. 1 (1999): 110–26; J. L. Casti, *Complexification: Explaining a Paradoxical World through the Science of Surprise* (New York: Abacus, 1994); C. S. Holling, "Understanding the Complexity of Economic, Ecological, and Social Systems," *Ecosystems* 4, no. 5 (2001): 390–405; and John H. Miller and S. E. Page, *Complex Adaptive Systems* (Princeton, NJ: Princeton University Press, 2007).

3. Parts of this argument in an earlier form can be found in the author's "Cybered Conflict" blog on the Atlantic Council website, www.acus.org/tags/cybered-conflict. The concept of security resilience is also much more extensively discussed in C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power and National Security.* (Athens: University of Georgia Press, 2011). On the term "cyberwar," see R. Hughes, "Cyber War: Bits, Bytes and Bullets," *The World*

Today 63, no. 11 (November 2007), www.chathamhouse.org/publications/twt/archive/view/167215.

4. Kenneth J. Knapp and William R. Boulton, "Ten Information Warfare Trends," in *Cyber Warfare and Cyber Terrorism*, ed. L. Janczewski and A. M. Colarik (New York: Information Science Reference, 2007).

5. M. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge, MA: MIT Press, 2002).

6. N. Kshetri, "Pattern of Global Cyber War and Crime: A Conceptual Framework," *Journal of International Management* 11, no. 4 (2005): 541–62.

7. Josh Rogin, "Attack by Korean Hacker Prompts Defense Department Cyber Debate," *Federal Computer Week Online*, February 9, 2007, http://fcw.com/articles/2007/02/09/attack-by-korean-hacker-prompts-defense-department-cyber-debate.aspx?sc_lang=en.

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

9. Isaac Porche, "Stuxnet Is the World's Problem," *Bulletin of the Atomic Scientists*, December 9, 2010, http://thebulletin.org/web-edition/op-eds/stuxnet-the-worlds-problem.

10. Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier: Version 1.4, February 2011," *Symantec*, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

11. John Leyden, "FBI 'Planted Backdoor' in OpenBSD—Break Out the Code Auditing Kit," *Enterprise Security*, December 15, 2010, available at *The Register*, www.theregister.co.uk/2010/12/15/openbsd_backdoor_claim/.

12. Michael J. Gross, "Stuxnet Worm: A Declaration of Cyber-War," *Vanity Fair*, April 2011, www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

13. M. Benedikt, *Cyberspace: First Steps* (Cambridge, MA: MIT Press, 1991).

14. Riva Richmond, "The RSA Hack: How They Did It," *New York Times*, April 2, 2011.

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

16. William Lynn, "Introducing US Cyber Command," *Wall Street Journal*, June 3, 2010.

17. John Markoff, "BIT: The Asymmetrical Online War," *New York Times*, April 3, 2011.

18. G. Morgan, *Images of Organization* (Santa Monica, CA: Sage Publications Inc., 2006).

19. Economist Staff, "The Future of the Internet: A Virtual Counter-Revolution," *Economist*, September 2, 2010.

20. Benedikt, *Cyberspace.*

21. J. F. Brenner, "Why Isn't Cyberspace More Secure?" *Communications of the ACM* 53, no. 11 (2010): 33–35.

22. Dan Goodin, "Upstart Crimeware Wages Turf War on Mighty Zeus Bot: All Your Bots Belong to Us," *El Register*, February 9, 2010; and A. A. Cárdenas, S. Radosavac, J. Grossklags, J. Chuang, and C. Hoofnagle, "An Economic Map of Cybercrime," Paper presented at the 37th Research Conference on Communication, Information and Internet Policy 2009, George Mason University Law School, Arlington, VA, September 2010.

23. C. Tilly, *Coercion, Capital, and European States, Ad 990–1992* (Cambridge, MA: Blackwell, 1992).

24. Elinor Mills, "Insecurity Complex: In Their Words: Experts Weigh in on Mac vs. PC Security," *CNET online*, February 1, 2010, http://news.cnet.com/8301-27080_3-10444561-245.html?tag=contentMain%ntentBody;1n.

25. Louise Comfort, Arjen Boin, and Chris Demchak, eds., *Designing Resilience: Preparing for Extreme Events* (Pittsburgh: University of Pittsburgh Press, 2010).

26. John Leyden, "Monster Botnet held 800,000 People's Details: Fourth Zombie Admin Could Be in South America," *El Register*, March 4, 2010, www.theregister.co.uk/2010/03/04/mariposa_police_hunt_more_botherders/.

27. Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Ecco Books, 2010).

28. G. Todd, "Cyberlaw Edition: Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition," *Air Force Law Review* 64, no. 65: 65-211.

29. S. J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law* 27 (2009): 192.

30. Richard Baskerville, "Hacker Wars: E-Collaboration by Vandals and Warriors," *International Journal of e-Collaboration* 2, no. 1 (2006): 16. doi:10.4018/jec.2006010101.

31. P. Gao, "Using Structuration Theory to Analyze Knowledge and Process Management in a Consortium: a Case Study," *Knowledge and Process Management* 14, no. 2 (2007): 104-16.

32. Joseph Nye Jr., *The Future of Power in the 21st Century* (Cambridge, MA: Public Affairs, 2011).

33. John Leyden, "DNS Made Easy Rallies after Punishing DDoS Attack: 50Gbps of Botnet-Powered Badness," *The Register*, August 9, 2010, www.theregister.co.uk/2010/08/09/dns_service_monster_ddos/.

34. R. Young, "Hacking into the Minds of Hackers," *Information Systems Management* 24, no. 4 (2007): 281-87.

35. Shane Harris, "The CyberWar Plan, Not Just a Defensive Game," *National Journal*, November 14, 2009.

36. K. J. Knapp and W. R. Boulton, "Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments," *Information Systems Management* 23, no. 2 (2006): 76-87.

37. Tanjug, "Libyan Opposition Accuses '50,000 Serb hackers,'" *B-92 News*, March 24, 2011, www.b92.net/eng/news/society-article.php?yyyy=2011&mm=03&dd=24&nav_id=73415.

38. Josh Rogin, "Cyber Officials: Chinese Hackers Attack 'Anything and Everything,'" *Federal Computer Week Online*, February 13, 2007, http://fcw.com/articles/2007/02/13/cyber-officials-chinese-hackers-attack-anything-and-everything.aspx.

39. Jennifer Baker, "EU and US join NATO Cyber Security Pact," *Computerworld UK online*, November 23, 2010, www.computerworlduk.com/news/security/3249914/eu-and-us-join-nato-cyber-security-pact/.

40. D. H. Bayley, *Patterns of Policing: A Comparative International Analysis* (Piscataway, NJ: Rutgers University Press, 1990).

41. R. L. O'Connell, *Of Arms and Men: A History of War, Weapons, and Aggression* (London: Oxford University Press, 1989).

42. C. S. Gray, "How Has War Changed since the End of the Cold War?" *Parameters* (Spring 2005), 14-26, at 21.

43. Note that the former West Germany did retain an interest in national resilience as a Cold War frontline state but, nonetheless, strongly separated its military from the internal decisions of the society. Its national leaders have assigned national-level protections in cyberspace to the Ministry of Interior with little to no role for the national security services of the Ministry of Defense, whose role in cyberspace is solely to protect its own classified networks.

44. F. P. Harvey, "The Homeland Security Dilemma: Imagination, Failure and the Escalating Costs of Perfecting Security," *Canadian Journal of Political Science/Revue canadienne de science politique* 40, no. 2 (2007): 283–316.

45. Gil Ariely, "Knowledge Management, Terrorism, and Cyber Terrorism," in *Cyber Warfare and Cyber Terrorism*, ed. L. Janczewski and A. M. Colarik (New York: Information Science Reference, 2007).

46. Stephen Walt, "Is the Cyber Threat Overblown?" in *International Security*, ed. J. Joyner (Washington DC: Atlantic Council of the US-New Atlanticist).

47. See, for example, the International Convention on Cybercrime as amended 2006. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT = 189&CM = 8&DF = 17/02/2006&CL = ENG.

48. Cheryl Pellerin, "DOD, DHS Join Forces to Promote Cybersecurity," *American Forces Press Service US Department of Defense*, October 13, 2010; and D. E. Bambauer, "Cybersieves," *Duke Law Journal* 59, no. 3 (2009): 377–595.

49. Ellen Nakashima, "Pentagon's Cyber Command Seeks Authority to Expand Its Battlefield," *Washington Post*, November 6, 2010.

50. William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010; Government of France, "The French White Paper on Defence and National Security," Office of President Nicolas Sarkozy (Paris: Govournement de France, 2009); and Richard Norton-Taylor, "The UK Is Under Threat of Cyber Attack, the National Security Strategy Says—Home Secretary Outlines Priority Threats Facing Britain ahead of the Publication of the National Security Strategy Today," *Guardian Online*, October 18, 2010.

51. J. Rollins, and A. C. Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations" (Washington, DC: CRS, March 10, 2009), www.fas.org/sgp/crs/natsec/R40427.pdf; and Thom Shanker, "Pentagon Will Help Homeland Security Department Fight Domestic Cyberattacks," *New York Times*, October 20, 2010.

52. DOD, "Department of Defense Strategy for Operating in Cyberspace," July 14, 2011, www.defense.gov/news/d20110714cyber.pdf.

53. The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011, www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.