Building a Comprehensive Strategy of Cyber Defense, Deterrence, and Resilience

Tim Ridout

INTRODUCTION

Interest in deterrence for the cyberspace domain is high in the United States. The increasing incidence and severity of a variety of malicious cyber activities, primarily over the Internet, highlights the need for more comprehensive strategies for deterring various forms of cyber conflict. To this end, this article .discusses concepts, terms, and situations to facilitate strategic dialogue, and also offers a set of guiding principles for cyber strategy itself.

The technical specifics and complexity of the cyberspace domain make strategic discussions particularly difficult, and mental frameworks tend to be oriented toward analogies from nuclear deterrence concepts. Although a lexicon for cyberspace is emerging, gaps and conceptual confusion remain. Vague references to data security, cyber weapons, and cyber warheads do not illustrate conflict dynamics in cyberspace particularly well. At the same time, a set of common terms and concepts simplifying

Tim Ridout *is a fellow at the German Marshall Fund of the United States, where he focuses on political and economic issues in Brazil, in addition to global security challenges. Prior to joining GMF, he worked at Institutional Shareholder Services as a corporate governance analyst, primarily studying Brazilian companies. Before that, he was a program manager with the Brazil-U.S. Business Council at the U.S. Chamber of Commerce. Ridout regularly contributes to the Huffington Post, and his writing has also appeared in the* Boston Herald, Christian Science Monitor, Hartford Courant, *and* Providence Journal. *He received his master's degree from the Fletcher School of Law and Diplomacy in 2011.*

terms are valuable for effective communication among the political, legal, engineering, business, law enforcement, and military communities, as well as the general public.

Different imperatives drive and inform the terminologies of the communities above, shaping their problem-solving approach. Law enforcement is driven by the need to gather sufficient evidence for successful prosecutions in the court system, highlighting questions of probable cause and evidence-gathering methods. Engineers necessarily focus on precise measurement of physical realities, analytically subdividing the world into trillions of unique pieces. Political and military communities tend to focus on big-picture and strategic questions, keeping their attention on top-level effects and outcomes, since their analyses must account for complex national, international, and global social dynamics. Lawyers tend to have a level of precision to their thinking that makes them similar to engineers; given that language and law are inextricably linked, linguistic precision is as important to lawyers as physical precision is to engineers. For the business community, efficiency, innovation, and profitability are foremost in their minds, meaning that they are driven to constantly improve and seek new opportunities; they tend to be concerned about questions of predictability, liability, and cost. For these different professional communities and the general public to truly be able to communicate, they have to engage with each other and learn a common lexicon. Mutually understood vocabularies are essential in order to debate conflict scenarios and possible responses to them with an eye toward weighing costs and tradeoffs, unintended consequences, legality, potential for escalation, and likelihood of success.[1]

Reaching a more stable strategic situation with reduced conflict in cyberspace requires debating, architecting, constructing, communicating, and learning a framework that de-incentivizes various forms of cyber conflict and counters potential first-use of cyberspace to cause mass destruction, but which also involves preparing to continue operations and return to normal as quickly as possible when attacks are successful (i.e. —resilience). Resilience has already been highlighted in the 2015 U.S. Department of Defense Cyber Strategy and frequently emphasized by Commander of Cyber Command Admiral Rogers, computer security experts, and others. However, cyber resilience has not been given much treatment in the inter-

Cyber resilience has not been given much treatment in the international security literature, and the concept has not reached the mystical status that deterrence enjoys.

national security literature, and the concept has not reached the mystical status that deterrence enjoys.

Many cyberspace concepts demand clarification. A few critical ones are discussed here along with an illustration of cyber conflict scenarios. These top-level concepts seek to subsume within static terms a host of lower-level technical and tactical intricacies that are continuously evolving, and there are countless detailed engineering and human questions that lie behind these terms when it comes to architecting, operating, and engaging with cyberspace. A comprehensive cyberspace strategy in peacetime should include a combination of defense, deterrence, and resilience as guiding elements; deterrence by itself will not produce the desired results, so cyber strategy needs to be multifaceted and adaptive.

CRITICAL CYBER CONCEPTS

Building on the work of John Sheldon and Daniel Kuehl, I define cyberspace as: "a global domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to capture or create, store, modify, exchange, and exploit information via interdependent and interconnected networks to produce kinetic and information effects."[2] While the electromagnetic spectrum exists independently of cyberspace, when electronic devices are transmitting to each other through the electromagnetic spectrum, the transmission itself can be considered part of cyberspace.

It is important to note that the Internet and cyberspace are not precisely the same thing: the Internet is the primary modern means of networking electronic systems, but there are other forms of networked electronics that do not use the Internet. What makes the Internet both valuable and disruptive is that computers linked via the Internet have two-way capacity, enabling people all over the world to communicate, send, and receive large amounts of information, and remotely cause kinetic effects more easily than in the case of other networked electronics. The Internet Protocol, which enables a specific and widespread way for networked electronics to "talk" to each other, combined with root servers that store lists of unique names and numbers for each electronic device with an IP address, are among the most relevant engineering aspects that differentiate this particular part of cyberspace from the rest. Other networks use the Internet Protocol, but they are physically disconnected (or "air-gapped"), from the Internet and do not use its root servers to organize and direct traffic. TV satellite dishes that receive video transmitted from outer space

in analog or digital form are part of cyberspace, but they tend not to be able to transmit back to the satellites and tend not to be connected to the Internet, although they can be designed that way.

Kinetic Effects and Information Effects

I define information effects as the outcomes produced by electronic networks and systems whose intrinsic value is to create situational awareness, enable communication and coordinated human action across distances, generate and distribute actionable knowledge, and otherwise store and exchange all kinds of information that are of direct utility as presented to the human senses in the form of sounds or visuals. By contrast, I define kinetic effects as those outcomes produced by electronic networks and systems whose intrinsic value is to give commands to robots and appliances, operate machinery and vehicles, adjust energy flows within human-made systems, and otherwise create physical motion and impact.

These are not meant to be rigid categories, but rough delineations of different top-level effects. Electronic devices are continuously performing internal functions that are both informational and kinetic: they employ interacting components and electrical currents to move electronic data packets and signals that contain information and allow for its communication with other electronic devices and the human senses.

In fact, most computer systems and networks that produce kinetic effects will by necessity also produce information effects. For example, an apartment building heating system that is run by a computer-and-sensor network could be set on fully automated mode to produce a kinetic effect of continually adjusting furnaces, fans, and vents to keep the temperature stable in the building's units. In order to do that, it also needs to be able to continuously measure the temperature through its sensors, capturing the information presented by the world and translating it into numerical representations that have meaning to humans as well as the rest of the networked system. The system also has to be able to receive the initial input temperature desired by the human operator—perhaps 68 degrees Fahrenheit / 20 degrees Celsius. In this instance, the information effects of measurement and communication to the rest of the system are directly linked to the kinetic effects of giving operational commands to the heating system that produce motion and consume energy.

By contrast, many computer networks and systems are designed solely to produce information effects and do not produce kinetic effects. While networked computers allow for the physical transmission of information

through space via email, this is an information effect: for example, I was able to work on this article at my stationary home computer, my mobile laptop in various coffee shops, and my stationary work computer. Emailing the drafts to myself allowed me to access the same *information* in multiple locations as the article evolved. If I wanted to create the kind of kinetic effects discussed above, however, I could download software and link my laptop to a networked thermostat and heating system, which would allow me to give operational commands remotely from my laptop to that system. Technically speaking, transporting the information contained in electronic data packets from one computer to another involves kinetic functions and interacting components within networks and devices, but the intrinsically valuable output is the information effect, not the kinetic functions.

Zooming out to a greater distance, a satellite in outer space might not be connected to the Internet or even use the Internet Protocol, but it is still part of cyberspace. In the case of a television satellite, it produces the information effect of streaming video to subscribers around the world. When the operator wants to reposition it in its orbit, it sends commands via radio waves that produce the kinetic effect of activating the satellite's thrusters to move it to a new location in orbit. Whereas many electronic devices transmit information using electronic data packets, many satellites and other devices transmit information in analog fashion—i.e., by modulating the frequency or amplitude of radio waves. Signals that produce kinetic effects tend to be heavily encrypted, sent on a separate frequency, and sent to an electronic system on the satellite known as the "bus." Signals producing the information effects of streaming video to satellite dishes on Earth travel on a different frequency, tend not to be encrypted, and are sent to and from an electronic system on the satellite known as the "payload." It is possible to "harden" signals by physically altering them, but encryption and authentication of signals are among the most important for security. Although these aspects have technical and engineering significance, a tactical perspective is primarily concerned with the speed with which these signals travel through the electromagnetic spectrum, whether they enable specific devices to "talk" to each other, and how easy it is to intercept, decode, spoof, and otherwise disrupt these signals.

Law and policy are primarily concerned with the top-level impact of kinetic and information effects. For example, if someone hacks into the computer systems of a self-driving car and acts to produce the ultimate kinetic effect of turning on the windshield wipers for 10 seconds (and nothing else), the rider may be briefly confused but do nothing about it. However, if the hacker is an assassin who takes control of the entire

car and produces the kinetic effect of driving it off a cliff, law enforcement and lawyers would likely get involved to find out what happened and why. If a state actor or a group of anarchists hacks into the networks of the global financial system and acts to produce the information effect of altering the account balances of millions of people and companies—thus causing widespread economic confusion, costly legal proceedings, and social turmoil—the international community would likely take steps to punish those responsible.

Cyberspace vs. Information Space

Internationally, there is conceptual confusion and political disagreement over how to manage the technical, physical aspects of cyberspace and how to deal with the information effects that it produces. The two are inextricable, but a better understanding of both terms would improve strategic dialogue. Although all nations are concerned about both information and kinetic effects, leaders from countries with less permissive attitudes toward freedom of expression are concerned about the disruptive social effects of free information flows, such as cultural change, unrest, and violent revolution. As such, they often make reference to *information space* in addition to *cyberspace*. Questions about managing information space are increasingly relevant in the United States and elsewhere with regard to terrorist recruitment, child pornography, criminal syndicates, etc., but the term itself is not commonly used.

Cyberspace could be said to "create" information space as we know it today, while also producing myriad kinetic effects apart from information space.

It is therefore important to clarify that cyberspace is the entirety of the physical, technical domain created by networked electronics and their transmissions through the electromagnetic spectrum. By contrast, information space can be conceptualized as the sum total of the information effects produced by cyberspace. Thus, cyberspace could be said to "create" information space as we know it today, while also producing myriad kinetic effects apart from information space. Despite political disagreement over how to treat them, both are useful and complementary concepts that are important for domestic and international strategic dialogue.

Electronic Data vs. Data

In computer science terms, data does not mean precisely the same thing as its traditional understanding of "factual information (as measurements or statistics) used as a basis for reasoning, discussion, or calculation."[3] Electronic digital data packets flowing through networks have an electrical signal and move at up to the speed of light. Electronic digital data and analog electronic signals that create kinetic effects are not useful to conceptualize as factual information even though they contain information and have their own factual reality in the simplest sense that they exist.

When it comes to conversations about "data security" and "data privacy," it is important to differentiate between the raw materials of electronics and computer science on the one hand, and factual information on the other. They sometimes overlap, but not always. To make such a differentiation in strategic conversations, I refer to electronic data to mean any and all electronic digital data packets held in the form of ones and zeroes as well as electronic analog signals, while retaining *data* in its traditional meaning in order to avoid confusion. This terminology would require adding "electronic" to the terms *data at rest* and *data in motion*, which FBI Director Jim Comey frequently refers to in explaining the difference between electronic data that resides on computers and electronic data that is flowing through networks, whether wireless or wired. The distinction between electronic data at rest and electronic data in motion is itself a useful conceptual shorthand. From the perspective of technical engineering and tacticalmaneuvering, whether they are analog or digital, how they are encoded, whether or not they are encrypted (and how strongly), the specific networks and electromagnetic spectrum through which they travel, and their speed are essential to understand in order to take actions that produce desired effects.

ILLUSTRATIONS OF CYBER CONFLICT

There are countless ways to gain unauthorized access to computer networks and systems in order to cause an effect, whether informational or kinetic. Malware, short for malicious software, is the most common catch-all term for computer code that achieves a specific effect that the malware creator wants, but the system owner does not. Depending on the magnitude of the effects, malware could also be considered a cyber weapon. Malware can usefully be broken down into three main components: the propagation method, exploit, and payload. As Trey Herr frames the components of malware,

> A Propagation Method (Pr) is the means by which malware is inserted into a target network or system, such as an infected USB stick or email carrying a compromised attachment. An Exploit (E) is code designed to compromise some aspect of a software system which allows third parties to effect unintended operations or consequences. A Payload (P) is the code with a malicious purpose whose delivery and execution are the goals of any piece of malware.[4]

Modern computer systems and networks have many complex, interacting components, hardware, and software, and so there are guaranteed to be holes in systems that can be exploited to gain access. Errors in the millions of lines of software code enable actors to cause unintended effects. The components themselves can be compromised at the point of manufacture. Legitimate users can be tricked into granting access. A covert agent or criminal may have access to a building with sensitive systems and plug in a USB or other physical object to gain access. Creative operators are constantly devising new ways to break into continuously evolving systems. The "Internet of Things"[5] is expanding, more machines and vehicles are being computerized and connected, and societies are becoming increasingly reliant on cyberspace. This means that the attack surface—the multiplicity of access points as well as the multitude of different software programs running on systems—is vast and growing. New operating systems, software, and updates could create new vulnerabilities or repair old ones. Hackers often wait for companies to release patches via the Internet to repair vulnerabilities in software and operating systems, at which point they rush to write malware that exploits the now-public vulnerabilities before users have downloaded and installed the patch, presenting a security challenge during those windows of risk. These and other factors mean that cyberspace is a continuously shifting landscape.

Cyberspace is a continuously shifting landscape.

Once actors gain access to an unfamiliar computer network, they have to map the system. This could take months or years, depending on how complex the system is, how similar it is to well-known systems, and what effect the intruders want to have. During this process, the intruders might prepare the battlefield or lay the groundwork for a future operation by injecting lines of code throughout the system. As their knowledge of the intricacies of the system and the human administrators grows, they may prepare malware that will be likely to succeed in giving commands or taking control of parts of the system and producing certain intended effects.

In the course of normal system updates and patching software flaws, the exploits that the intruders used may be rendered obsolete. But intruders tend to steal legitimate login credentials as soon as they first gain a foothold in the system and then use those to gain access subsequently, making the activity appear like normal network traffic. Moreover, they could find new vulnerabilities and write new exploits if the stolen credentials become obsolete.

Depending on how stealthy and sophisticated the intruders are, as well as how sophisticated and vigilant the defenders are, these operations may be discovered and neutralized. If information-sharing about threat indicators is robust, packet sniffers that analyze electronic data packets as they enter and pass through the network may have immediately alerted the defender's administrators of a malicious intrusion. The defender may choose to divert the intruder to a honey pot, a decoy system that allows the defender to monitor the operational behaviors without the intruder's knowledge, in order to figure out what the intruder is after and what it might have already done in the network. If the defender has access to a skilled computer forensics team and trained detectives, the defender may also be able to attribute the intrusion to specific people and groups, opening the option of retaliation.

In political and legal terms, whether to refer to specific operations as cyberattacks, cyber theft, cyber manipulation, or some other iteration will depend on the effects or the intended effects—if and when they become known. But at the level of bits, bytes, and electronic data packets, it is common to refer any and all malicious system penetration and disruption as cyberattacks. The situation dynamics lend themselves to speaking in terms of attackers and defenders, as if each electronic data packet were a soldier trying to breach the city walls of the computer network perimeter. Although this terminology is helpful for a discussion of system and network dynamics, it is important to note that an actual attack has not occurred until the "attacker" has produced negative kinetic and/or information effects that reach a certain point. It is helpful to think in terms of two "levels"—the "internal network" level and the "real world" level. The "internal network" level has its own unique conflict dynamics that resemble a never-ending game of hide-and-seek, with attacking forces continuously trying to stealthily probe, penetrate, and cause harm while defending forces try to monitor, lead astray, and expel, with detection being the hardest part. Once detected, expelling attackers is relatively easy. This occurs *within* running networks and systems, only comprehensible to those with sufficient technical expertise. The "real world" level includes the

effects, human operators, the surrounding environment, and the physical objects such as microchips or hard drives that could be smashed to pieces with a hammer if you get frustrated enough with the whole enterprise.

In the case of a live cyberattack, if the attackers are successful in preparing the battlefield and the payload is already dormant in the target system, it then becomes a question of when to initiate the attack sequence. Doing so could be as simple as opening the program on the attacker's command-and-control server that controls malware and activates the payload on the defender's system, and then hitting return; by this point, the attacker has unleashed electronic data packets moving at up to the speed of light on their way to the target, almost like the fuse of a bomb. In an automated cyberattack, the rest of the attack is self-executing: the attacker simply has to sit back and hope that the intended effects are achieved. In a directed cyberattack, the attacker must continue to make decisions about which functions on the target system to perform, in what order, and at what speed, with electronic data packets flowing back and forth between the defender's system and the attacker's system with each new command. Currently, most malicious activity appears comprised of directed cyberattacks.

If the defender becomes aware of the operation in real time and suspects it is a directed cyberattack that is not yet complete, the possibility of shutting off all transmission capability may exist as a blunt instrument to neutralize the attack. The defender could also take actions to neutralize within its systems while still allowing back-and-forth transmission, perhaps trying to back-trace it to the source in order to begin attributing it. Depending on the sophistication and resources of both sides relative to each other, the attacker's capacity to maintain anonymity, and for how long, could vary considerably.[6]

Cyberattacks involving logic bombs—malware that, once implanted by a human operator, is set to self-execute at a specific time or when certain conditions are met at the internal system level—do not even require a human to initiate the attack sequence. More complicated still are autonomous cyberattacks, perhaps involving autonomous polymorphic malware,[7] that no longer have active human involvement and that continue to rove about, rather than lying in wait like logic bombs. Here, "polymorphic" means that this malware keeps altering subtle parts of itself such that its functionality does not change but its signature may change infinitely. This makes autonomous polymorphic malware harder to detect than known malware; it is analogous to dangerous background radiation that is simply "out there in the ether."[8] Attributing autonomous cyberattacks could be

prohibitively expensive, and trying to retaliate against them could lead to self-inflicted harm through mistaken identity and by creating perceptions of a reckless defender lashing out randomly.

There is also a host of cyber operations that do not involve directly accessing electronic systems. Distributed Denial-of-Service (DDoS) cyber operations are one such Internet-specific instrument in the cyber conflict toolkit. Rather than gain access, they simply overwhelm the target systems' bandwidth and computing resources by flooding them with requests for information through electronic digital data packets. These tend to be carried out using botnets, constellations of potentially millions of computers that hackers have compromised with malware and can direct using command-and-control servers. Most people, however, will not realize that they are part of a botnet because their computer will appear to function normally, perhaps running a bit slower than normal. The malware essentially allows the command-and-control server to piggyback on each computer's bandwidth and computing capacity to carry out coordinated actions from multiple locations such as DDoS attacks. Using the sheer volume of electronic data in motion through the Internet as a tool of conflict to render servers inoperable is tactically similar to other instruments such as radar noise jamming, though the technical means of accomplishing the are different.

Though the engineering differences between cyber conflict tools such as radar noise jamming and DDoS operations are significant, from a tactical effects-based perspective, both are forms of overloading electronic devices through a flood of signals sent via the electromagnetic spectrum to the point where those devices are rendered temporarily inoperable. Although the U.S. military currently distinguishes radar jamming as a tool of electronic rather than cyber warfare, the significant overlap in tactical effects (as well as the existence of U.S. Cyber Command) suggests the need to harmonize electronic warfare operations and cyber operations. After all, most electronic devices are networked to at least one other device through the electromagnetic spectrum. Among the relevant ontological differences within these areas of activity are whether operators are using cyber to control their

Although the U.S. military currently distinguishes radar jamming as a tool of electronic rather than cyber warfare, the significant overlap in tactical effects (as well as the existence of U.S. Cyber Command) suggests the need to harmonize electronic warfare operations and cyber operations.

own weapons systems and communicate through their own networks; interfering with a portion of the electromagnetic spectrum in some way or overloading an adversary's transmission capabilities; collecting electronic data in motion from public networks, both wired and wireless; or directly penetrating an adversary's electronic systems and networks to cause an effect. Whether the catchall term becomes *cyber* or *electronic warfare*, avoiding mental, linguistic, and bureaucratic compartmentalization could boost creativity by allowing operators with similar skill sets and conceptual frameworks to interact.

Offensive cyber operations could have the ultimate information effects of depriving users of access to the information on their electronic devices until ransom is paid; destroying information to set back a competitor; stealing and publishing mass amounts of sensitive information in order to tarnish reputations; stealing specific, high-value information such as advanced weapons designs; providing detailed situational awareness and actionable insights for the sake of intimidating or killing specific people; and so on. They could also produce the kinetic effects of crashing an airplane in flight; sabotaging manufacturing plants; crashing a swarm of miniature drones into high-value targets; and driving a car into a crowded marketplace, to name a few.

This is a small slice of conflict situations and concepts. The complexity and breadth of cyber conflict scenarios is vast and will require creating more terms to describe how cyberspace can be instrumentalized to achieve objectives. In so doing, it will be important for the computer engineering community to take the time to explain new technologies and tools, while avoiding using new words to describe variations on the same thing, such as when "software programs" became "apps." An app could be considered one of many *types* of software programs, or they could be explained as different organized collections of computer code, or some other iteration, but it is important not to change terms unless something meaningful has changed. Committing to relatively static top-level terms is critical for effective communication in the interest of making law and policy, even as technical and tactical sub-categories within each term grow and multiply to keep up with evolving technology.

BUILDING AND COMMUNICATING A COMPREHENSIVE CYBER STRATEGY

Moving Beyond Analogy

It is important not to be trapped by the conceptual frameworks of the past. They can provide useful insights into resolving novel problems, but rigidly applying specific doctrines and policies from one domain and

set of tools to another can blind us to the key differences between domains. The concept of deterrence has been reified (and with good reason) as a strategy for avoiding catastrophic nuclear war, and it affects the thinking of strategists who came of age during the Cold War. But deterrence alone is not a silver bullet in the case of cyber strategy.

Nuclear deterrence is premised on the assumption of massive retaliation and guaranteed second-strike capabilities in order to make the first use of nuclear weapons unappealing for policymakers, who might otherwise contemplate a nuclear strike to gain an advantage over an adversary. Mutually Assured Destruction became shorthand for this deterrence logic. In contrast to the still-evolving cyber frameworks, nuclear deterrence logic is underpinned by capabilities as well as articulated processes and responses: nuclear powers have created warheads, delivery mechanisms, hardened siloes and mobile platforms, early warning and monitoring capabilities, secure launch procedures, crisis hotlines between militaries and heads of state, varying postures and levels of readiness, etc. This allows actors to make threats credible, check potential moves and countermoves, and provide for de-escalation mechanisms in the nuclear deterrence framework. To reach a sense of strategic stability, however, this framework first had to be debated, architected, constructed, communicated, and learned. As noted in the introduction, stabilizing and reducing conflict in cyberspace likewise requires debating, architecting, constructing, communicating, and learning a framework that de-incentivizes various forms of cyber conflict and counters potential first-use of cyberspace to cause mass destruction. This framework, however, must also involve preparing to continue operations and return to normal as quickly as possible when attacks are successful.

Stabilizing and reducing conflict in cyberspace likewise requires debating, architecting, constructing, communicating, and learning a framework that de-incentivizes various forms of cyber conflict and counters potential first-use of cyberspace to cause mass destruction.

Deterrence is appealing in the nuclear context because the actors are states with clear "return addresses"; it is much easier to identify the source of an attack, and the consequences of even one successful strike could be catastrophic, depending on the target. Moreover, the effects would be immediate and irreversible. Nuclear warheads are designed for concentrated massive destruction and cannot be used for other purposes, except

when threateningly wielded in order to gain influence.[9] By contrast, cyber conflict and crime run the gamut from petty theft and targeted manipulation all the way up to mass disruption and destruction, whether by potentially taking down the electric grid or causing chaos in the financial system for extended periods. The threat environment is further complicated by the multiplicity of state and non-state actors that can have an impact, combined with the difficulty of attributing malicious cyber activities to specific people and groups. And though certain effects of large-scale cyberattacks would be felt immediately, their impact tends to accumulate over time the longer the affected systems are inoperable, damaged, or performing the wrong functions.

For example, being without electricity for two days is potentially dangerous for some people, but is merely an inconvenience for most. However, losing electricity for a month or two could lead to a significant number of deaths through starvation, disease, and exposure to the elements. If loss of electricity also means losing access to potable water, depending on how the water system is designed in a given city, even two days without electricity could be dangerous if residents do not have stored water. The ultimate effects will vary depending on context and duration.

Additionally, the assured ability to deliver any given high-impact or "strategic" cyberattack is questionable and subject to the whims of the continuously shifting landscape of cyberspace. As Patrick Cirenza notes, "If a network administrator patches vulnerabilities in the target computer code, or an agent is unable to insert a USB drive to cross an air-gapped system, then a strategic cyber weapon that was deliverable yesterday might not be today."[10] Moreover, explicitly revealing malware-based cyber weapons renders them obsolete because the defender can then repair system vulnerabilities. Wielding these types of cyber weapons as a convincing threat would probably require first demonstrating highly sophisticated successful attacks in the real world, while claiming or implying that these are simply a starting point. The greater ambiguity surrounding the effects that can be achieved by any given cyber threat makes "strategic" cyber weapons trickier to rely on for stability.

Of course, an electromagnetic pulse (EMP) attack would be more assured to have the desired effects of damaging or destroying all electronics within a certain range, which becomes an increasingly impactful weapon as the "density" and reliance on cyberspace grows. Considered part of electronic warfare, EMP attacks could be conceptualized as attacks *on* cyberspace itself, rather than attacks that travel *through* cyberspace in the form of malware or jamming.

The potential effects that can be achieved via cyberspace vary considerably depending on the functions performed by a given device or system and the machinery it may control; the presence or not of redundant alternatives; and the relative ability of the device, system, and machinery to return to normal functionality quickly, if at all. Moreover, there are so many different ways to gain access to computer networks and systems through ever-evolving means, with varying degrees of stealth and anonymity, and which are available to myriad state and non-state actors, that it is impossible to prevent all forms of cyber conflict. Therefore, resilience should be a core piece of the overall strategy.

Thinking Through Deterrence and Resilience in the Cyber Context

Deterrence can be presumed successful anytime a state or non-state actor chooses not to engage in theft, blackmail, coercion, or any action intended to cause material harm, death or destruction via cyberspace out of fear of attribution and punishment. Paul Davis has usefully disaggregated "deterrence by denial" from dissuasion, establishing that

> 'Deterrence' is sometimes given even broader meanings that include offering reassurances and inducements on the one hand or trying to compel action on the other. Such indiscriminate usage undercuts discourse. I reserve 'deter' for the classic meaning that involves threat of punishment. I also refer to 'dissuasion by denial,' rather than 'deterrence by denial.'[11]

I consider dissuasion to primarily be part of cyber defense efforts, although categories describing human psychology tend to blur at the edges and should not be taken as wholly distinct phenomena.

When it comes to resilience, it is crucial to distinguish between the resilience of networked electronic systems themselves and the resilience of critical infrastructure functionality and society writ large. Focusing on networked computer and electronic systems, Paul Nicholas explains that, "While there is no internationally accepted definition of 'cyber resilience' there is a growing consensus that cyber resilience can be defined as the ability of complex cyber systems to continuously deliver the intended outcome despite chronic

It is crucial to distinguish between the resilience of networked electronic systems themselves and the resilience of critical infrastructure functionality and society writ large.

stressors and acute shocks."[12] I take a broader view, conceptualizing resilience as plans and actions that minimize damage, provide for continued operations, and facilitate return to full functionality as quickly as possible when cyberattacks are successful, whether they only affect computers and networks themselves or also have broader information effects such as undermining the integrity of the financial system or kinetic effects such as harming machinery, vehicles, and critical infrastructure. This returns to the distinction between the "internal network" and "real world" levels, seeking to combine both levels in the concept of resilience.

Focusing on the architecture of computer networks and systems, William Bryant argues, "The virtue of cyberspace resilience lies between rigid conformity to a single system that can be taken down with a single attack on one side and complete chaos within an unworkable mess of a network on the other. A reasonable middle ground for cyberspace operators is to select a handful of different, well-designed operating systems and then implement them throughout their networks."[13] He also stresses the need to reduce attack surfaces and react dynamically to attack.[14]

Another useful perspective on cyber resilience is offered by Bob Walder and Chris Morales: "Organizations should assume the breach will occur and proactively seek to reduce the impact of that breach. That is the key to cyber resilience. True cyber resilience allows organizations and governments to continue to operate and provide services for clients or citizens in the face of persistent and never-ending attack. Instead of trying to stop attacks in cyberspace or even at the network perimeter, networks must become resilient so they continue to function regardless of the level of attack."[15]

Regarding the electric grid, among the most important networked computers for industrial functions are supervisory control and data acquisition (SCADA) systems. Tom Fanning, a U.S. electric utility CEO, recently noted that if SCADA systems operating the grid were taken offline in the United States, "We can run the system manually."[16] Thus, even if the "internal network" level fails the "real world" level could continue, albeit with greater physical exertion and higher cost. Putting plans in place and training personnel for manual operation of critical infrastructure in the event that a significant cyberattack is successful are a key piece of resilience. Another aspect of resilience can be seen in the U.S. Navy's resumption of training in celestial navigation—such as through the use of sextants—in the event that the global positioning system (GPS) is rendered inoperable through cyberattack.[17] In a simpler form, resilience could include keeping hard copy printouts of regularly used files and important records, ensuring that redundant non-Internet communications systems such as landline tele-

phones are retained, or planning to have enough cash on hand if ATMs go down for a couple of days or more. Incorporating differentiation, variation, and diversity into our lives builds resilience. Having multiple options for accomplishing the same goals makes it harder for adversaries to throw our lives into disarray. Complete homogeneity and centralization are vulnerabilities. Anyone who has felt the intense panic of losing their primary laptop or smartphone that has not been backed up knows this viscerally. Resilience planning can be done at the individual, family, firm or organization, city, state, national, and global levels—in both the public and private sectors.

Knowing that you are resilient may not scare an adversary, but it will make you less fearful if you and your people are confident that you can continue to operate and will quickly return to normal if an attack is successful. It will also buy time for decision-makers to accurately attribute (if possible), and retaliate (if appropriate). Depending on whether it is a state or non-state actor, retaliation may take various forms and the time between the initial attack and the retaliation may vary.

Deterrence through the credible threat of punishment must play a role in the strategic framework for managing and preventing cyber conflict, but emphasizing it over resilience would be a mistake because its effectiveness is limited by the sheer volume of cyber conflict, ambiguity about culprits, and the prohibitive costs of attempting to punish each and every malicious incident. Moreover, the potential for misattribution or intentional framing by a third party makes retaliation a riskier option. Relying on a posture of assured, immediate retaliation is untenable.

When there is sufficient evidence and punishment is deemed necessary to boost deterrence of future cyberattacks by demonstrating that there are real costs associated with such activity, it should be proportional and transparently applied, while protecting certain sources and methods. Economic sanction and arrest are already tools that the U.S. government explicitly uses to deter certain kinds of malicious cyber activity, but in cases of what could be considered significant consequences, it is safe to assume that retaliation would not be constrained to specific methods and would be undertaken "in a place and time and manner that we choose."[18] As defined in the U.S. Department of Defense Cyber Strategy, "significant consequences may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States."[19]

In the case of a successful, significant terrorist attack via cyberspace, the response would likely be to identify and pursue the group or individuals responsible, patiently picking the organization to pieces through

robust international law enforcement and military partnerships, monitoring capabilities, machine learning, and discriminating precision, operating within the confines of the law. The ideal is to arrest those responsible, but lethal force inevitably would also be used, especially in weak states where legitimate authorities lack capacity. These responses would require an accompanying strategic communications campaign to explain efforts to both U.S. and global publics as well as to discredit the terrorist narrative.

It is essential that both deterrence and response methods account for and seek to minimize negative repercussions and unintended consequences—both in the potential for escalation, and in the harm caused by excessive surveillance to free expression, creativity, innovation, and rule of law.

Information effects that rise to the level of significant consequence, whether maliciously perpetrated by state or non-state actors, represent one of the biggest challenges in security strategy. For example, the theft of mass amounts of sensitive information has the potential to cause cause impacts that humanity has only recently had to contemplate because the speed and scale now possible due to modern cyberspace have changed the nature of the threat. Crafting a response to such incidents when there is confidence in attribution is a new area of strategic thinking that will require creativity, game theoretic models, and cautious experimentation, all while being attentive to signals from other countries and feedback loops.

Additional deterrence tools should be made available to policy makers in an effort to change the cost-benefit analysis of malicious cyber attacks, but not before potential for escalation and unintended consequences are carefully considered with the difficulty of attribution in mind. It is essential to design tools and methods that account for and seek to minimize the harm caused by excessive surveillance to free expression, creativity, innovation, and rule of law.

Finally, resilience could play a critical dissuasive role by reducing the utility of cyber offense, especially when joined with the credible threat of punishment. If you demonstrate that you can absorb a blow, bounce back quickly, and then hit back, resilience and deterrence can be a potent combination. The psychology of deterrence could be considered offensively minded, whereas the psychology of resilience could be construed as defensively minded. Although state actors can likely be deterred from undertaking cyberattacks of significant consequence, certain non-state

actors such as terrorist groups cannot be assumed to be deterrable, making resilience an essential aspect of strategy when defense and deterrence fail.

Cyber Defense is an Equally Important Part of Overall Strategy

On the defensive side of the equation, this is where efforts have been focused and cyber defense remains critically important to strategy. This primarily involves a set of engineering, educational, training, and resource allocation solutions to keep computer and other electronic networks and systems from being penetrated by unauthorized actors. Penetration testing and red teaming are important aspects of boosting defenses. Improving system design with human error and intentional deception in mind from the beginning is important. Mechanical switches that can enable and disable certain functionalities only through physical access could reduce the possibility of remote monitoring and manipulation when those functionalities are not being employed by the legitimate operator. Educating the public, sharing threat indicators, and continuously monitoring nefarious activity to adapt defenses and stay one step ahead are essential. In addition to keeping intruders out, strong network defenses are likely to have dissuasive effects on less sophisticated actors, but determined and well-resourced actors (advanced persistent threats) will be capable of penetrating systems. For these actors, a combination of deterrence and resilience could reduce the instances of, and harm caused by, malicious cyber activity.

CONCLUSION

The discussion above suggests a model upon which to base future strategic debates surrounding technologies that revolutionize warfare and human society more broadly. No meaningful discussion of costs, tradeoffs, unintended consequences, escalatory potential, and strategic purpose can occur unless the cyberspace discussion employs a mutually understood vocabulary that distills general principles and concepts into useful shorthand, while remaining faithful to the technical and engineering realities of the technologies themselves. This requires investing time in patiently learning and discussing the technologies as well as the changes they have wrought to interpersonal, intergroup, and international conflict dynamics. The political, legal, engineering, business, law enforcement, and military communities in particular must develop mutual vocabularies in addition to engaging in discourse with the general public.

Based on the understanding that cyberspace is a continuously shifting

landscape with myriad actors, a range of consequences, and significant possibility for stealth, a comprehensive strategy for managing cyberspace during peacetime needs to be multifaceted and adaptive. In order to reduce the number, severity, and duration of malicious cyber activities, strategy should be based on elements of defense, deterrence, and resilience. ***f***

ENDNOTES

1 This conclusion is drawn from the author's ongoing research. For more detail, see Tim Ridout, "Here We Go Again: A Comparative Approach to Developing Cyberspace Governance Frameworks," in Damien van Puyveld (ed.), forthcoming.

2 See Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Kramer, Starr, and Wentz (eds.), *Cyberpower and National Security* (Washington, DC and Dulles, VA: National Defense University Press and Potomac Books, Inc.), 28 and John Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* (Summer 2011): 95-112, http://www.au.af.mil/au/ssq/2011/summer/sheldon.pdf.

3 "Data," *Merriam-Webster Dictionary*, <http://www.merriam-webster.com/dictionary/data> (accessed March 14, 2016).

4 Trey Herr, "PrEP: A Framework for Malware and Cyber Weapons," *Cyber Security Policy and Research Institute Report* (March 2014). <http://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/54ee0d97e4b0621e861ba345/1424887191756/PreP+paper.pdf> (accessed April 5, 2016).

5 The "Internet of Things" is a marketing term used by many corporations to refer to electronic devices—typically with sensors that capture information from the world—that are embedded in objects such as refrigerators, chairs, robotic manufacturing assemblies, electric "smart" grids, toasters, etc. and which are connected to the Internet or another Internet Protocol-enabled network. The term focuses attention on machine-to-machine communication and automated processing of electronic data to improve efficiency and autonomy. In reality, the Internet has always been connected to "things," so it will be important to continue to clarify terminology and construct an intelligent discourse surrounding this marketing concept.

6 Tim Ridout, "The Strategy of Anonymity in Cyber Conflict: An Analytical Framework," *XI Conference of Forte de Copacabana International Security* (October 2014): 95-112 <http://www.kas.de/wf/doc/kas_39113-1522-2-30.pdf?141010195940#page=95> (accessed April 5, 2016).

7 Angela McKay, "International Norms in Cyberspace: A Discussion with Minister Marina Kaljurand," Conference at the Center for Strategic and International Studies, Washington, DC, December 18, 2015, <http://csis.org/event/international-norms-cyberspace-discussion-minister-marina-kaljurand [at 35:20]> (accessed April 5, 2016).

8 The author thanks Marc Hutzell for this articulation.

9 Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), find page.

10 Patrick Cirenza, "The Flawed Analogy Between Nuclear and Cyber Deterrence," *Bulletin of the Atomic Scientists*, February 22, 2016, <http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179> (accessed April 5, 2016).

11 Paul Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *New York University Journal of International Law and Politics* 47(2) (Winter 2014): 333, <http://nyujilp.org/wp-content/uploads/2015/11/NYI203.pdf> (accessed April 5, 2016).

12 Paul Nicholas, "Working to Increase the Cyber Resilience of Cities Around the Globe," *Microsoft Cyber Trust Blog*, February 11, 2016, <http://blogs.microsoft.com/cybertrust/2016/02/11/working-to-increase-the-cyber-resilience-of-cities-around-the-globe/> (accessed April 5, 2016).
13 William Bryant, "Resiliency in Future Cyber Combat," *Strategic Studies Quarterly* 9(4) (Winter 2015): 91.
14 Ibid., 104.
15 Bob Walder and Chris Morales, *Analyst Brief: Cyber Resilience* (Austin, TX: NSS Labs, Inc., 2014), <https://www.nsslabs.com/index.cfm/_api/render/file/?method=inline&fileID=C0FED81D-5056-9046-93A24B68A52C3A75> (accessed April 5, 2016).
16 Patrick Tucker, "The Ukrainian Blackout and the Future of War," *Defense One*, March 9, 2016, <http://www.defenseone.com/technology/2016/03/ukrainian-blackout-and-future-war/126561/> (accessed April 5, 2016).
17 Lily Hay Newman, "Naval Academy Brings Back Celestial Navigation Training in Case of a Cyberattack on GPS," *Slate,* October 19, 2015, <http://www.slate.com/blogs/future_tense/2015/10/19/u_s_naval_academy_reinstates_celestial_navigation_education.html> (accessed April 5, 2016).
18 David Sanger, Michael Schmidt, and Nicole Perlroth, "Obama Vows a Response to Cyberattack on Sony," *New York Times*, December 19, 2014, <http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html?_r=0> (accessed April 5, 2016).
19 *The Department of Defense Cyber Strategy* (Washington, DC: U.S Department of Defense, April 2015), 5, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed April 5, 2016).