Atlantic Council

STRATEGY PAPERS

A Nonstate Strategy for Saving Cyberspace

Jason Healey

Foreword by Jeff Moss

A Nonstate Strategy for Saving Cyberspace

Atlantic Council Strategy Paper No. 8

Atlantic Council

Atlantic Council
1030 15th Street, NW, 12th Floor
Washington, DC 20005

ISBN: 978-1-61977-445-2

Cover art credit: Museum of Fine Arts of Rennes. Paysans surpris par un orage (Peasants Surprised by a Storm) by Francesco Giuseppe Casanova, ca. 1770.

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council, its partners, and funders do not determine, nor do they necessarily endorse or advocate for, any of this report's particular conclusions.

January 2017

Table of Contents

Foreword

Our lives are under attack, but because it happens mostly in the shadows, many people do not notice, leaving only the experts a chance of defending themselves. As we continue to blindly connect nearly all aspects of our lives into the foundation of the Internet for increased convenience, we are also increasing the chances that our day-to-day livelihood will be greatly disrupted or deleted.

At the personal level, that potential would be heartbreaking: bank accounts, family photos, music, contacts—all up for grabs. At the government level: public opinion, our nation's secrets, our ability to fight wars, our infrastructure that governs everything from highways to space—all vulnerable and subject to seizure or subversion by our enemies, state and nonstate alike.

I have seen this firsthand. At the Internet Corporation for Assigned Names and Numbers (ICANN), I was the chief security officer, helping to ensure that the Internet can continue to provide massive benefits to billions without much government oversight. I also saw the vulnerabilities of the Internet during the conferences I founded and organized like DEF CON and Black Hat. The underlying Internet we depend on for our social, cultural, economic, and individual empowerment is nowhere near secure enough to hold what we are building on top of it.

For these reasons, this *Atlantic Council Strategy Paper* that Jason Healey offers, "A Nonstate Strategy for Saving Cyberspace," is important. He recognizes that the Internet "may have surpassed Johannes Gutenberg's printing press as history's most transformative invention," and therefore must be acknowledged as such and protected. Following his advice—ensuring that "defense" surpasses "offense" in cyberspace—is the only way to protect the shared dependencies of the Internet so that it continues to provide great benefit to all people of the world.

I asked Jason to share his vision of this social dilemma we face at the DEF CON conference in 2014, and since then I have only seen more reasons to be concerned and heed his call to action.

This will of course come with challenges. The Internet is amazingly complex and surprisingly fragile, and its failure modes are impossible to predict. No one owns it, which is both its greatest strength and greatest weakness. It "was built on trust, not security," as Jason says, so as trust declines around the world, so does our confidence in the Internet's reliability.

At this crucial time in world affairs, the Internet will become more important than ever. This makes it imperative that we secure the Internet and all of cyberspace from the many threats it faces every second of every day. We need transparency matched with accountability, with solutions rooted not with states, but in the vibrant nonstate community working every day to keep the Internet safe and resilient. This all begins with an acknowledgement that the current trajectory of offense far exceeding defense is internationally destabilizing and ultimately unsustainable.

If public- and private-sector leaders are worried about the ways we live and work online—which they should be—then there is no better place to start solving the problem than by reading this *Atlantic Council Strategy Paper*. Only by realizing how much we have to gain by safeguarding the Internet from those who want abuse it for short-term benefit can we preserve and expand all the progress the United States, and humankind, has made so far.

Jeff Moss

Jeff Moss
Senior Fellow, Cyber Statecraft Initiative,
Brent Scowcroft Center on International Security,
Atlantic Council;
Former Chief Security Officer,
Internet Corporation for Assigned Names and Numbers (ICANN)

Executive Summary

America's future, and that of other nations and peoples, will be most secure in the long term with an emphasis on future prosperity unlocked by the Internet.

The Internet may have surpassed Johannes Gutenberg's printing press as history's most transformative invention, because of how it has spawned parallel simultaneous revolutions across other technologies. By making information so cheap to produce, compute, and share, the Internet enabled rapid advances in technologies as far afield as manufacturing and genetics.

The problem is that there is no guarantee that the future of the Internet, and the larger entirety of cyberspace, will be as rosy as its past. It is possible, even likely, that the Internet will not remain as resilient, free, secure, and awesome for future generations as it has been for current ones.

Imagine that twenty years after the invention of the printing press, the pope and the princes of Europe—in fact, anyone who had some basic skills and desire to do so—had the ability to determine exactly what was being printed, exactly who was printing it, and exactly to whom they were sending it. Worrying about intellectual-property theft, privacy, or civil rights (had those concepts existed) would have missed the bigger picture. With no trust in the underlying communication medium, the future of Europe and the future of humanity would have been profoundly changed—not just for five years, but for five hundred. If the printing press were as easily compromised as computers today, could there even have been a Renaissance or Enlightenment?

This amazing transformative technology, the Internet, is unsustainable without sweeping changes. People are becoming absolutely dependent on an unknowably complex system, where threats are growing far faster than the Internet's own defenses and resilience. The Internet is under grave threat from data breaches (e.g., Target and Home Depot), theft of commercial secrets (like the blueprints to the F-35 Joint Strike Fighter), the opportunity for widespread disruptive attacks (the digital takedown of Estonia in 2007 or of Sony in 2014) and systemic failures (the Heartbleed and Shellshock vulnerabilities), the erection of sovereign borders (the Great Firewall of China), and mass surveillance (as Edward Snowden's revelations demonstrated). For example, the Heartbleed and Shellshock bugs, discovered in 2014, affected underlying Internet technologies. These technologies, in turn, were only part of a vast technological system with countless subcomponents. Every part of that system is vulnerable.

Hence, a disruption to any one of them might ripple through the entire system via hyper-complex interactions, a situation which will become orders of magnitude worse with the coming Internet of Things (IoT).[1]

As President Barack Obama has said, cyberspace is a lawless "Wild West."[2] Because the Internet was built on trust, not security, it is easier to attack others online than to defend against those attacks. This is a decades-old trend, dating back to at least the late 1970s.

If the attackers retain the advantage over defenders year after year, then, over time, the Internet could pass a tipping point. At that point, the Internet would become far less useful and critical than it is today. Perhaps someday soon, there will be too many predators and not enough prey.

Unfortunately, when it comes to cyberspace, governments pursue contradictory ends. On the one hand, they want to protect the prey—Internet users—in order to enhance prosperity. But, on the other hand, this end is clearly outweighed by their ability and willingness to be voracious predators, to use the Internet as a means to attack those actors they see as working against their national interests.

Therefore, if we are not careful, the metaphor for cyberspace will go from bad (the Wild West) to worse (Somalia). Every time efforts are made to secure the Internet, there is (and will be) some new threat to drag it down into chaos, with devastating consequences for the United States' cyber-dependent economy, and those people who have come to cherish their online lives.

Technologies that seem so promising today, such as online voting or the smart grid, might never materialize if, together, the world cannot overcome these security challenges. Future generations may look back and wonder why anyone would feel safe buying something online, or how online videos survived without quickly getting hacked.

How many future Renaissances or Enlightenments will never occur, simply because we treated the Internet as a place for crime, spying, and warfare ("everyone does it," after all), rather than the most innovative and transformative product of human minds in five hundred years? Will society soon reach "peak Internet?"

The reason why this state of affairs came about is because the Internet is a type of global commons. All actors benefit from protection of the commons, but all actors also have an incentive to abuse it. Governments are often the only actors that can sustainably protect and defend commons. Yet, at the same time, governments also often abuse the commons to push their own national security interests in a zero-sum fashion. The result is the degradation of the commons itself. Although the commons analogy is not perfect, it nonetheless works because it highlights a contradiction between protection of a public good (the safety and integrity of the Internet for innovation and the economy) and a Hobbesian security dilemma (the perceived need to use the Internet for military and intelligence purposes in a dangerous world). This contradiction is at the heart of the problem.

The only way to ensure cyberspace remains as free, resilient, secure, and awesome for future generations is to flip the historic relationship between attackers and defenders of the Internet. We should give those who have an interest in protecting cyberspace an advantage over those who want to use it to attack others (or the Internet itself). This idea of making cyber defense easier than offense can be summed up with a simple formula: **D > O.**

Giving cyber defenders the advantage over the offense is imaginable with new technology, policy, and practice that are applied patiently, internationally, at scale, and with the private sector at the fore. It is not imaginable if nations continue to escalate large-scale espionage or mass surveillance, subvert cyber companies, engage in shadowy wars against real adversaries, or coerce former satellite states.

Prosperity for the United States and the global economy is only assured if the United States and like-minded nations, civil society, and other nonstate actors all work toward a goal of making defense easier than attack.

At the same time, nonstate actors (not least the IT and cybersecurity companies themselves) are increasingly powerful. However, just as fishermen might deplete a fish stock to maximize short-term profits at the expense of the fishery itself, corporate interests do not always align with their own longer-term economic interests. The best public policies must shape the situation to get the best out of both governments and nonstate actors, to become stewards of humanity's most dynamic creation and create a sustainable cyberspace.

Highlights of This Paper

Current US cyber policymaking is characterized by a number of shortcomings:

1. there is no single US digital strategy, so no way to balance competing priorities
2. longstanding and increasing militarization of cyber policy, with the Department of Defense (DoD) as the main player, rather than an agency that focuses on innovation and the economy, such as the Department of Commerce
3. misunderstanding of the dynamics of cyber conflict
4. persistent short-term view of US national security thinking
5. overestimation of the effectiveness of public-sector action to solve cyber problems
6. lack of attention to the central problem: that the Internet remains offense-dominant and could be far worse than it is today

7. an unpreparedness for global cyber shocks

To address these shortcomings, the United States must build a strategy centered on **a sustainable balance in US government decision-making,** a strategy built around three key ends:

> **Advancing Prosperity**: First and foremost, US policy must ensure that cyberspace and the Internet advance US and global prosperity, not least through continuous and accelerating innovation. Other priorities are important but subordinate.
>
> **Being Emblematic of the United States and Its Values**: Cyberspace and the Internet are US inventions, reflecting US values, though they are used in all nations and by all generations. US policy should cherish this opportunity for soft power and be careful not to squander this astounding once-in-a-generation national advantage.
>
> **Providing New Tools for Pursuing Traditional National Security**: Of course, US military and intelligence agencies must use these new technologies as well, not least because the world is becoming more dangerous and unpredictable. However, these technologies need to be developed and used with extreme caution when they conflict with other goals, especially America's long-term, Internet-fueled prosperity.

To meet these objectives and advance prosperity, US policy should pursue two overlapping goals: 1) make the Internet **defense dominant (D > O)**, so cyber defenders have the advantage, and 2) add a time component to security concerns by aiming for a **sustainable cyberspace**. The goal is not just better computer security today, but an Internet that is as safe, resilient, and awesome for future generations as it was for its pioneers.

Together, these goals define the large-scale vision that should drive an American **nonstate-centric strategy**. The only way to achieve a sustainable defense-dominant Internet is to build a strategy around the private sector, the United States' true cyber power, and other nonstate actors. Few, if any, major Internet crises have ever been decisively resolved by any government. Rather, nonstate actors like cybersecurity companies, major technology companies, and volunteer response groups have played the key role. As argued in *Dynamic Stability*, the first *Atlantic Council Strategy Paper*, US leaders must become more comfortable playing a multilevel game, working with nonstate actors "who possess a greater range of capabilities than at any time in history."[3]

A successful cyber strategy must therefore accept this central role for nonstate actors and the private sector, and then work outward from that core US strength. Wherever possible, solutions to governance, regulation, protection, and response must stem from this core.

Creating a sustainable cyberspace, where defense has the advantage over offense, will be extremely difficult, but still possible with actions like the following:

1. improve US strategies and internal processes
2. sow the seeds for disruptive change
3. prioritize solutions that scale
4. develop grants to extend nonstate capabilities
5. regulate for transparency, not security
6. focus on systemic risk and resilience for the long term
7. look beyond a security mindset to sustainability.

Text Box 1: Glossary

Key terms:

Internet: The global interconnected information network that uses a particular technical standard, TCP/IP, to communicate. In practice, "Internet policies" tend to deal with issues like connectivity, broadband access, innovation, and other social or economic issues.

Cyberspace: This report uses the term to mean a larger whole, encompassing not just the Internet, but also all network-connected devices and global interconnected information technologies generally, regardless of the actual means or standards used.

Cyber: The term had been reserved just as a modifier (see below), but now has taken on a life of its own, to generally mean the same as cyberspace. However, in usage, especially in the military or in national capitals, "cyber policies" have come to mean those that deal with cyber crime, national security, warfare, and espionage.

IT and ICT: These terms are roughly interchangeable. IT for "information technology" is the preferred term in the United States, while ICT is internationally more common, to more broadly include "information and communications technologies."

Text Box 1: Glossary (cont'd)

Other related terms:

Cybersecurity: Essentially, the same as "computer security," dealing with the integrity, availability, and integrity of computers, networks, systems, and information.

Cyber conflict: When nations and nonstate groups use offensive or defensive cyber capabilities to attack, defend, and spy on each other, typically for political or other national security purposes.

Cyber war: Actions, usually by a nation-state, to damage or disrupt another nation's computers or networks. Attacks so heavily damaging that the effects are similar to those achieved with traditional military force, and they are considered to be an armed attack. So far, despite millions or billions of cyberattacks and dozens of cyber conflicts, there has not yet been a true cyber war.

Cyber crime: A criminal act that is mediated through cyberspace, in which computers or networks play an instrumental role, such as stealing credit card numbers or other personal data.

Cyberattack: Geeks, cops, spies, and soldiers all have varying definitions, but, in general, this includes any deliberate, illegal, disruptive, or spying attempt against a computer, network, or information. That is, a distributed denial of service or intrusion.

Intrusion: Any deliberate and illegal entry into a computer system, such as to exfiltrate (steal) information or conduct a later disruptive attack.

Exploitation: A term of art meaning stealing information from a computer, but not causing any disruption, which is considered an attack. Usually, "exploitation" is used to specify an act of espionage, rather than a mere criminal theft of data.

DDoS: A distributed denial-of-service attack. The attacker uses a command-and-control system to control anywhere from a few computers or a few million computers, to overwhelm the bandwidth or resources of another computer system, with the intent to disrupt operations.

Malware: Malicious software, such as viruses, worms, or Trojan horses, used to gain access to or damage a computer, network, or information.

Everything Depends on the Internet… but the Internet is Threatened

The Internet, and ICT and cyberspace more broadly, has driven unprecedented innovation and prosperity—and near-total dependence on a system both unfathomably complex and inherently insecure. This complexity will become magnitudes of complexity more severe with the addition of billions of devices connected through the Internet of Things (IoT).

It is widely known that the ICT revolution has been driven by the doubling of capability every few years, as exemplified by Moore's Law, but often overlooked is how this doubling has fed revolutions in biology and manufacturing. The societal and economic gains from three-dimensional (3D) printing, robotics, unmanned aerial vehicles, genome mapping and gene therapies, and biobricks are all dependent on a robust ICT infrastructure, due to ever-faster computing and more capable networks, able to get data around the world seemingly instantaneously.

"Digital economy" is a deeply misleading term. It leads one to think of ordering books online or using a credit card to reserve a hotel room from a travel website. This misses the real story, the *digitized* economy. In fact, a recent report by the Atlantic Council and Zurich Insurance Group, which modeled the economic impacts of ICT, found that these technologies could add perhaps *$180 trillion to global GDP through 2030*, a staggering sum that far outpaces the $20 trillion in losses due to cybersecurity problems.[4]

The gains of being connected are significantly higher than the losses, because the Internet and ICT have been resilient over time, thanks to a combination of stable technology, dedicated technicians, and proven resistance to random outages. It was designed to be so, with robust underlying standards, routers, cables, and switches that are quite reliable, and which have minor consequences when they do fail. There are also legions of hard-working technicians for whom it is a matter of pride to keep their systems—and the Internet—running, all day, every day.

Yet, even a few decades are a relative blip in humankind's experience with such a complex technology, so this brief history might reflect a short-term trend rather than a permanent state. This system is not just amazing and complex; it is also fundamentally insecure.

Text Box 2: The Dawn of IoT

If you think cyberspace is insecure today, just wait for the coming Internet of Things. The first five billion devices (servers, workstations, mobile devices) will not be like the next fifty to five-hundred billion. Modern cars are computers on wheels, and cutting-edge patient care is delivered over the Internet—each of these examples may involve dozens or hundreds of specialized computing devices. If the world gets this right, the promise will transform society; if not, it will eliminate the resilience society seeks. While impacts to dataflows, intellectual property, and personally identifiable information (PII) are costly, cybersecurity failures in the Internet of Things will also be measured in human life, and shattered trust in markets and governments. Approaches to securing these devices must also be differentarmed attack. So far, despite millions or billions of cyberattacks and dozens of cyber conflicts, there has not yet been a true cyber war.

While ICT has so far been resilient enough, the increasingly tight coupling of the Internet with the real economy and society means this might not last. A full-scale cyber shock is far more likely to occur than most Internet professionals care to admit. Quite literally, no one in the world understands the massively complex interconnections of ICT, within itself and with the physical world. And, increasingly, ICT failures or attacks can cascade directly to Internet-connected banks, water systems, cars, medical devices, hydroelectric dams, transformers, and power stations. The Wild West anarchy which has occurred over the networks might take those networks down with it.

Past Internet incidents and attacks have only disrupted software or wrecked things made of silicon. These can be recreated or replaced with relative ease. As the Internet connects with real life, in places like the smart-grid interconnection with the electrical-power infrastructure, this will no longer be true. With the Internet of Things, incidents will break objects made not just of silicon, but of concrete and steel, of industry and industrial objects, and not just commerce.

As expressed by computer-security expert Dan Geer, "[a]s society becomes more technologic, even the mundane comes to depend on distant digital perfection."[5] In such a world, cyberattackers may be able to have far more lasting and damaging impacts, a future the Internet called a "Clockwork Orange Internet," which could "cost the world nearly USD 90 trillion of potential net economic benefit" to 2030.[6]

Text Box 3: The Economy's Dependence on the Internet Has Been Long Recognized

It has become fashionable to say that economic dependence on the Internet has only happened recently, or that the issue has only recently become recognized as a top-tier priority for policymakers. In fact, there is a long history of recognition of these matters:

"Computers have become such an integral part of American business that computer-related risks cannot be separated from general business risks."
National Academies of Science report, Computers at Risk (1991)

"The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are...increasingly reliant upon certain critical infrastructures and upon cyber-based information systems."
Presidential Decision Directive 63 (1998)

"Our economy and national security are fully dependent upon information technology and the information infrastructure...that today connects millions of other computer networks making most of the nation's essential services and infrastructures work."
National Strategy to Secure Cyberspace (2003)

"The globally-interconnected digital information and communications infrastructure known as 'cyberspace' underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security. This technology has transformed the global economy and connected people in ways never imagined."
White House Cyberspace Policy Review (2009)

"Digital infrastructure is increasingly the backbone of prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies."
White House International Strategy for Cyberspace (2011)

"The internet is revolutionizing our society by driving economic growth and giving people new ways to connect and co-operate with one another. Falling costs mean accessing the internet will become cheaper and easier...'democratizing' the use of technology and feeding the flow of innovation and productivity."
UK Cyber Security Strategy (2011)

One of the key reasons the future of the Internet is at risk is **the continuing attacker and offense advantage over defense**: attackers have a far easier time trying to break into a computer than the defenders have trying to keep them out (call it O>D for easier reference).

Many companies today use a "red team," or penetration testers, to try to break into their online systems to improve security. One rule of thumb is that "[f]ew if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought." Worryingly, that quote was written in 1979, and it remains true today.[7] Not only the "red teams," but also the attackers, have enjoyed the advantage in cyberspace for more than thirty-five years, even in the infancy of the Internet, even before the World Wide Web. The system, even though it has so far been resilient enough as a whole, enables misbehavior. As old industrial-control systems are connected to the Internet, they are nearly indefensible.

Four Key Failures

Attackers have had an easier time than defense, owing to at least four key failures: Internet architecture, software weaknesses, open doors for attackers, and complexity.

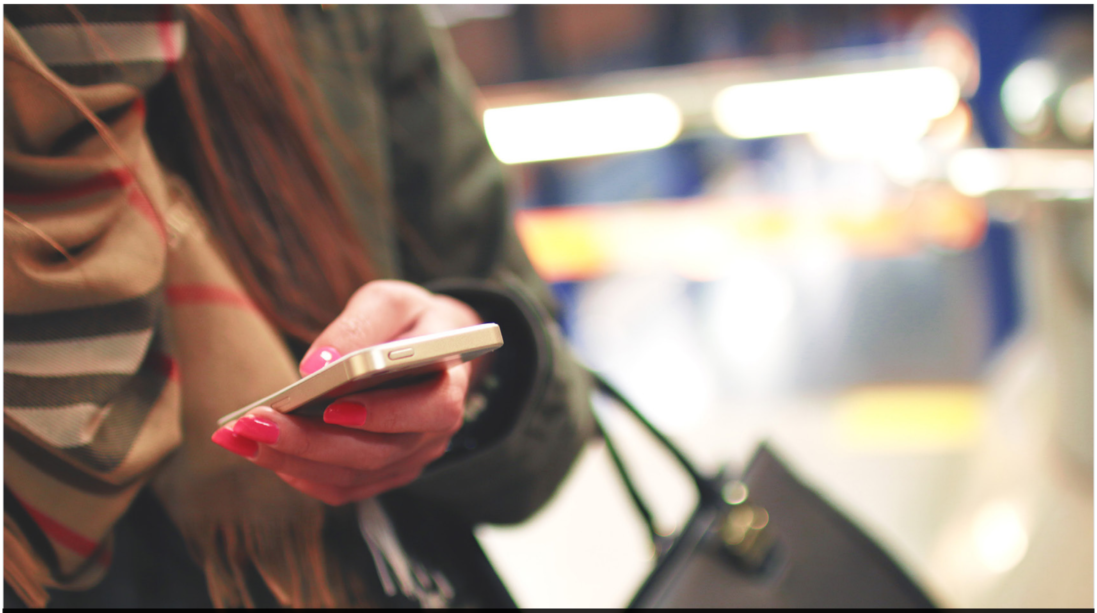
The early Internet was designed with few rules, other than to ensure computers and networks could interconnect. After all, the participants knew one another and the impact of any misuse was minor, because the network was only used for research and academic purposes. Security started out as, and has continued to be, an add-on, tacked onto the system as an additional requirement rather than engineered from the beginning,

Software weaknesses are another key failure. Trying to add security after the product is launched is not a problem just for the Internet, but for software as well. This is not a new issue, as computer security expert Bruce Schneier summarized more than a decade ago:

> Today there are no real consequences for having bad security or having low-quality software of any kind. Even worse, the marketplace often rewards low quality. More precisely, it rewards additional features and timely release dates, even if they come at the expense of quality.[8]

Attackers also have an easier time because they can choose the weakest spots of the defense. Nearly twenty-five years ago, the *Computers at Risk* report first reported the overall impact of this imbalance: "the attacker must find but one of possibly multiple vulnerabilities in order to succeed; the security specialist must develop countermeasures for all."[9]

A fourth major reason for attacker advantage is the stunningly complex interactions of Internet systems (like the backbone routing system, corporate IT systems that connect to it, or even the arbitrary behavior of individual users and their governments). Such complex systems are dominated by "processes that can be described, but not really understood...often discovered



In both developed and developing nations, the direction of the Internet is being increasingly driven by the new generation of "Millennials," who are the first true digital natives. *Photo credit: JESHOOTS/ Pexels*

through trial and error, and what passes for understanding is really only a description of something that works."[10] If it can not be understood, it can not be properly defended.

Global Trends

Another risk to the long-term resilience of cyberspace is that **the Internet and ICT are facing daunting changes, including shifts in demographics, technology, and policy challenges**.

As more nations are coming online, they want a say in how the Internet is run and the values it embodies, while billions of people from developing economies are coming online with demands of their own.

In both developed and developing nations, the direction of the Internet is being increasingly driven by the new generation of "Millennials." The first true digital natives, they have grown up with the Internet, rather than the older generations whose formative years predated it. "Unlike baby boomers and Generation X," according to *Bloomberg*, "it's from the Internet that millennials derive their sense of freedom," and not from cars or other technologies that liberated their parents.[11]

Such newly empowered online citizens will respond differently to perceived threats, such as mass surveillance or military cyberattacks. Nations and companies that fail to adapt might experience unexpected blowback. To an intelligence agency or marketer, Facebook is a great collection resource; to a digital native, it can be as private as the bedroom and no business of anyone else.

Beyond the growth in people coming online, there is an even more massive uptick in both the number and kinds of devices due to the Internet of Everything, which will connect tens of billions of devices.[12] At the same time, there is a change in how people connect, with mobile devices increasingly prevalent, and changes in how and where computing is done (cloud computing and storage, wearable and embedded computers, and, in the medium term, quantum computing).

All of these devices are just one source in the huge growth of collected information—the trend called "Big Data"—with "enough information in the world to give every person alive 320 times as much of it as historians think was stored in" the famed Library of Alexandria.[13] Especially when stored in accessible cloud data centers, this data can be harnessed in ways never thinkable when it was on paper, storage tapes, or papyrus scrolls. Data analytics are finding ways to use this mass of data to solve complex social or commercial challenges (or to monitor and surveil people) in ways previously unimaginable.

Beyond these megatrends, there are more direct issues of technology itself and the broader intersection between technology and policy. Can Moore's Law hold indefinitely? Will battles over network neutrality, copyrights and patents, or other policy and legal issues drag the system backward?[14]

Loss of Trust

All of the above means that a last major risk to the long-term resilience of cyberspace is **that the Internet and ICT are facing a crisis over loss of trust and the role of governments**.

Paradoxically, even as more people come online and modern economies are dramatically increasing their dependence on it, the Internet is becoming less and less trusted. According to a global survey conducted in late 2014, nearly two citizens out of three were more concerned about privacy than they were a year earlier.[15] Similar numbers were afraid of hackers getting their personal or banking details, feared their own government was secretly monitoring them, or were concerned about state-sponsored cyberattacks against their own state institutions.

The reasons for these fears and lack of trust are as obvious as the headlines of the past few years: massive data breaches that expose the data of tens of millions of people at a time; intrusions into even the most heavily defended sites in the world, like the White House; disruptive attacks against energy and other infrastructure; states unleashing cyber capabilities against each other with seeming impunity, in attacks like Sony or Stuxnet; the Snowden revelations of massive surveillance; and widespread commercial collection of personal data by companies with opaque privacy policies.

This loss of trust is hard to tackle, because cyberspace and the Internet have very little governance structure, and what they do have is in the midst of turmoil.

Nations with different values than its American creators want a say on what the Internet should be like, what values it should reinforce, and how it should operate. The days when governments stayed relatively hands-off are over. The Internet is no longer a "borderless" place, as nations have insisted that sovereignty matters, and backed up that belief with diplomacy and force—such as locking up bloggers, online pornographers, or hackers who break local laws or mores.[16]

This insistence on state sovereignty might restrain the Internet from developing naturally, by imposing national borders that fracture the Internet. Instead of one international network, it could become more like national rail or phone networks, connecting separate "islands," each firmly under a government's control.[17]

Internet governance—the global system that keeps cyberspace operating from day to day and agrees to new technical standards for better Wi-Fi, for example—is in the midst of this tug-of-war over control of the future Internet. Will it remain true to its American liberal roots, or develop into a more controlled place, like it is in China or Russia today? Even US policy is split: the policies aligned with Internet freedom and an open and resilient network push for loose Internet borders, at the same time that law enforcement, military, and intelligence policies make a very distinct line between US citizens and companies—which have some protections, but can be forced into cooperation—and non-American ones.

If nations dig in behind defended digital frontiers, there may be little willingness to cooperate on stronger Internet standards or work together to contain global shocks. If the Internet faced a true shock, comparable to the financial crisis of 2008, it is simply not clear who would be in charge, or what levers could be used to mitigate the problems posed to the cyberspace or society.

Current US Cyber Policy and Its Challenges

Tied to these larger trends are several challenges specific to how US cyber and Internet policies have developed over the past fifteen to twenty years.

Current US Strategies and Policies

The United States government lacks a single strategy to provide guidance to its many diverse departments, which work on different aspects of cyber and Internet policies.

The result is there are **at least five separate sets of strategies or policies**—two for prosperity and innovation (Internet freedom and commercial aspects, including Internet governance), two for traditional national security (military and espionage), and one for criminal justice in between. Without an overarching strategy above all of these, there is no easy way to decide when there are competing public goods and competing priorities. Without an overarching strategy, accountability becomes even more difficult, as different bureaucracies work at cross purposes.

One of the many pernicious side effects is that "cyber" policies have, to some degree, become synonymous with national security and criminal justice, while "Internet" policies are those for prosperity and innovation. The most important new development is that, in the past several years, the US government has become increasingly open in discussing these policies, and is now clearly the most transparent large government when it comes to cyber issues.

Prosperity and Innovation Policies

The prosperity and innovation policies center, most of all, on maintaining an open and resilient Internet, in line with American values of fundamental freedoms, privacy, and the free flow of information. The International Strategy for Cyberspace, issued by the White House in 2011, is the most important document, with very specific goals and vision:

> The United States will pursue an international cyberspace policy that empowers the innovation that drives our economy and improves lives here and abroad...grounded in principles not just essential to American foreign policy, but to the future of the Internet itself.[18]

This strategy is the heart of the United States' stated policies, and advances goals such as norms of responsible behavior, resilience of the Internet as a whole, capacity building, and encouraging open standards and technological innovation. The only time it mentions words like "attacks" or "espionage" is when talking about malicious actions that *others* perpetrate on the United States and its allies. In part as a result of this White House position, US friends and allies were shocked after learning, through the Snowden revelations, that words did not always match deeds.

In this category, too, are the policies on international Internet governance and domestic technology issues, like broadband connectivity, innovation, health or energy IT, and trusted online identities.[19] These are usually overseen by the Department of Commerce, or similar civilian agencies.

Diplomatic Policies

The State Department has been pushing twenty-first century statecraft to leverage Internet-related technologies, like Twitter and Facebook, to be better at diplomacy. For this strategy, however, the more important initiatives are those focused on keeping the Internet free and secure.

For example, the United States is pushing both the Freedom Online Coalition of twenty-six countries, which "argues that narrow and distorted visions of the internet cannot be allowed to prevail. Freedom must win out over censorship," as well as the Alliance for Affordable Internet, to draw "on expertise from governments, the private sector, and civil society to assist policy makers in expanding access while keeping prices low."[20]

In a recent speech in Seoul, Secretary of State John Kerry laid out two sets of norms important to the United States; the first set tied to international law, the second an attempt to create better rules of the road on cyber offense and defense: "[T]he basic rules of international law apply in cyberspace. Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties."[21] He continued with specific norms:

> We also support a set of additional principles that, if observed, can contribute substantially to conflict prevention and stability in time of peace...
>
> First, no country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure.

> Second, no country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm.
>
> Third, no country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain.
>
> Fourth, every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way.
>
> And fifth, every country should do what it can to help states that are victimized by a cyberattack.[22]

These US norms are an important step, and long overdue, but still leave important questions unanswered—not least for critics who wonder how to square statements that forego "aggressive" attacks that might "intentionally disrupt another nation's critical infrastructure" with activities like Stuxnet.

Criminal Justice Policies

Fighting cyber crime has long been one of the top priorities for the Department of Justice.[23] This includes a wide set of crimes, from stalking to hacking, espionage to theft of intellectual property, as well as international components, such as working to train foreign police forces or bring other nations' laws up to international standards.

Often, such law-enforcement actions support innovation and prosperity policies, as they work to reduce sanctuaries of cyber criminals or terrorists who might use cyberspace for their own malicious ends. However, the methods used to pursue these ends can often undermine cyber defenses. The most recent example is the strong push from law-enforcement agencies for a backdoor or other access to encrypted communications.[24] While this is certainly a legitimate desire of law enforcement, it is not one that cryptographers and computer scientists know how to deliver, at least not without undermining encryption for everyone.[25]

Traditional National Security Policies

The two sets of policies for traditional national security are not as clear as those for prosperity and innovation, as they have been developed behind closed doors, in secrecy. However, the related policies for the military and espionage have gradually become more obvious, due to leaks and belated transparency.

Secretary of State John Kerry speaking at Korea University in Seoul, Korea, on the importance of internet freedom and cybersecurity on May 18, 2015. *Photo credit: US Department of State*

Regarding **intelligence**, the US position seems to recognize few, if any, limits to intelligence gathering; more or less everything is permissible, except US agencies spying on American citizens and the theft of intellectual property for commercial reasons.

For example, US diplomats were leading the fight to create norms that make Chinese economic espionage beyond the pale, while all along the National Security Agency (NSA) was infiltrating not just US adversaries, but allies as well. Because none of these operations crossed the lines of spying on US citizens, and no information was passed to companies, they were seen as playing by the rules.

Within Washington DC, and especially within the Pentagon, there are clear lines between intelligence and military cyber operations, split between "Title 50" and "Title 10," respectively. Unfortunately, since most US cyber espionage operations are conducted by the military-run National Security Agency, and by the same commander who oversees military operations, this distinction between military and intelligence is bound to be confusing to ordinary Americans, technologists, and US allies.

Until 2015, the main strategy for **military** use of cyberspace was the Department of Defense Strategy for Operating in Cyberspace of 2011, which mostly discussed how the department could better use cyberspace through better security, partnering with industry and international partners, and the like.[26]

As with the International Strategy for Cyberspace, this defense strategy left the impression that cyberattacks and espionage are solely actions perpetrated against the United States by wicked hackers, foreign militaries, and spies. About the closest the document got to confessing any interest in these activities for the United States was that the Defense Department must "ensure that it has the necessary capabilities to operate effectively in all domains: air, land, maritime, space, and cyberspace."

Fortunately, the newest Defense Department document, the DoD Cyber Strategy of 2015, is far more transparent, clearly stating the department's three primary cyber missions. The department must:

1. "Defend its own networks, systems, and information;
2. "Be prepared to defend the United States and its interests against cyberattacks of significant consequence; and
3. "If directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans."[27]

The current Pentagon policy might be summarized that, as the world's "essential nation," the United States must be able to defend itself and have all capabilities at its disposal, especially in the face of cyber attacks by foreign governments.

Challenges to US Cyber Policies

US policymaking has lately been displaying more agility, resilience, and transparency— the "ART" of strategy discussed in *Dynamic Stability*—but the challenges to these cyber policies remain daunting. There are seven major challenges to how the United States approaches cyberspace that, if left unattended, will likely result in growing dangers and increasing disruption in the digitized economy.

1. There is No Single US Strategy: Because there is no single strategy, the US government cannot easily balance when there are competing priorities, as there is no guide on how to decide between two colliding public goods. To illustrate, the United States wants a secure and resilient Internet, while keeping Iran from enriching uranium. Both are valid public goals that also appear unrelated. However, to pursue the latter goal, the United States has sacrificed much of the first. To subvert the Iranian enrichment program, the US government: subverted parts of Microsoft's Windows Update function, a critical part of keeping computers safe from hackers; forged digital certificates, one of the underlying trust mechanisms of the Internet; and helped create Stuxnet, the first truly destructive malicious software.[28] When Stuxnet mistakenly leaked out of the Iranian networks (and the story of its creation subsequently leaked to the press), it almost certainly encouraged other nations to pursue their own programs. It also led Microsoft and other American companies to view the US government as just another adversary against whom they must defend.

A more recent example can be seen in whether US technology companies should fully encrypt people's personal data, so that only the owner and no one else—not the companies and not the FBI—can access it. The director of the FBI, James Comey, has said that "[p]erhaps it's time to suggest that the post-Snowden pendulum has swung too far in one direction."[29] Without a single strategy from the president, how can agency officials know? Who can be held accountable when different parts of government pursue competing priorities, both feeling they are meeting the President's intent?

By comparison, if the Obama administration was faced with the option of pursuing major new investments in coal mining and coal-fired plants to create new jobs, how would they likely have responded? That administration wanted to balance a mix of energy sources with a clean environment. But a balanced policy does not mean accepting both equally, and President Obama clearly prioritized the environment and climate change (just as the Trump administration seems likely to take the opposite view). This clear priority made each individual decision much easier. This prioritization is exactly what has been lacking in cyber strategies, as presidents have wanted both cybersecurity and world-leading offensive, espionage and law enforcement capabilities long after it was clear it could not have both. The Donald Trump administration does appear to finally resolve this balance, in favor of hard power. Though it is not the decision recommended by this report, or by the larger cybersecurity community, it is a priority. If the Obama administration had more clearly pushed cyber defense over the offense, its legacy in this space might not be so easily unraveled.

2. Longstanding and Increasing Militarization of Cyber Policy: The military and intelligence agencies of the US government can classify their work away from public scrutiny and (compared to agencies working on digital innovation or cybersecurity) have significantly larger budgets, fewer interagency hurdles, friendlier oversight committees in Congress, more and better trained personnel, relatively mature bureaucratic processes, long-term planners, and risk-seeking leadership supported by lawyers who want to get to "yes."

There are estimates of "fewer than 1,500 [Department of Homeland Security] cyber professionals," even though that department is the overall US government cyber lead, "compared with 66,000 to 88,000 personnel" across the Department of Defense.[30] Now, the DoD is pushing even further to create a new Cyber Mission Force, with "over 6,100 personnel organized across 133 teams."[31]

The Internet agencies, supporting the stated US policies of Internet freedom and innovation, make do with few of these advantages. For example, the State Department has perhaps two or three dozen diplomats bravely trying to convince the world that, in the face of Stuxnet and the Snowden revelations, the United States indeed wants peace and an open, secure Internet.

The Pentagon is building this massive force because it can; there are few hurdles. But is this colossal investment of resources in line with actual national priorities?

This force of cyber experts will not improve the patent system or turbo-boost innovation, will not nurture new ICT companies, nor invent game-changing technologies. It will sit behind vault doors at military bases around the world, defending Defense Department and other US systems, and waiting for the order to attack.

The cumulative effect of this focus on the military and intelligence levers of power, for more than a decade, is that the United States' most important policies and actions are not backing innovation or prosperity, but warfare and espionage.

Other nations had already been exploring their own military options for cyberspace, but once they saw the Pentagon leaping ahead, they piled in as well. Now, Brazil, Japan, South Korea, Colombia, Iran, China, Russia, Norway, and Spain are getting in on the act; any self-respecting military needs to boast of having its own cyber organization.[32]

3. Misunderstanding of the Dynamics of Cyber Conflict: Because cyber policy has become militarized, it is dominated by muscular talk and action. For example, there is in the Defense Department a strong sense that a firm show of US cyber capabilities is needed to get other adversaries to back down. In short, the often-unstated assumption is that being feared in cyberspace leads to better national security outcomes.

Yet, there is strong evidence that, after being on the losing end of a cyber engagement (or even seeing others lose), nations seem likely to accelerate their own capabilities, counterattack, or both. If you cause fear in others, you may win tactical engagements. In the long run, however, it may not be a winning national security strategy, as it leads to worse real-world outcomes.

This is a classic security dilemma. Adversaries see each other building and using cyber capabilities—each fearfully trying to create a better security outcome, and instead entering a spiral of escalation, as each adversary perceives (perhaps correctly) the buildup as directed at them and strives to catch up. A specific policy to be feared might only swirl the spiral of escalation faster, higher, and, of course, more expensively.

Worse, according to Professor Bob Jervis, a security dilemma is "doubly dangerous" if the offense is dominant over defense and it is hard to distinguish offense from defense, such as in cyberspace. In this situation, "arms races are likely" and "incentives to strike first will turn crises into wars."[33] This is a very unstable situation, as each side is likely to escalate, perhaps even with non-cyber, kinetic means.

In fact, the situation may be even more unstable than merely doubly dangerous. Not only is it difficult to distinguish offense from defense, but from intelligence collection as well. As General Mike Hayden has said, once one has access to an adversary's computer, disruption is a "lesser included case" of exploitation.[34]

Worse, cyber conflict has very low barriers to entry. If one nation begins to use offensive, counteroffensive, or espionage cyber capabilities of any kind, it is relatively easy for other nations to gain and use similar capabilities.

This all makes it especially likely that using cyber capabilities for offensive purposes, and for their deterrence value, will spark imitation and counterattacks, causing an escalating spiral of conflict.

And, remember, cyber is not a closed game.

To cause fear in its adversaries, the United States is likely to cause fear in others, not least its own citizens. A policy of fear will create confusion in those overseas who thought the United States wanted a peaceful, free, and open Internet. To enact fear, the United States will likely have to continue to co-opt or coerce IT companies, weaponize their technologies, and conduct widespread monitoring on or through their networks. Being feared will likely cause havoc with policy goals for Internet governance.

4. Persistent Short-Term View of US National Security Thinking: Another symptom of militarization is that, lacking a single strategy, the default US cyber national security policy has become focused largely on short-term issues of hard power.

President Obama himself has presented the United States with a choice: "[W]e can either work together to realize [cyberspace's] potential for greater prosperity and security, or we can succumb to narrow interests and undue fears that limit progress."[35] US policy has often, unfortunately, put the country on the wrong side of this equation.

Because attackers have the advantage, the Internet allows nations to attack one another anonymously, and with impunity. Over the last fifteen years, the thinking of US military leadership and policymakers has evolved, seeing this not just as a fatal *risk* but as a must-seize *opportunity*. Two of the most successful defensive technologies ever—encryption and Windows Update to automatically patch Microsoft computers—both seem to have been tampered or interfered with to support US espionage operations or covert actions.[36] Rather than cherishing these treasures and ensuring they were trusted tools, the United States exploited them for important, but ultimately short-term, benefits.

Birdseye image of Silicon Valley taken on March 29, 2013. Silicon Valley, and American ICT companies more generally, are the nation's true cyber power. However, through its policies, the United States has coerced ICT companies to be tools of American espionage. *Photo credit: Patrick Nouhailler/Flickr.*

With relatively limitless online spying and emphasis on military use in cyberspace, the US government is putting America's longer-term economic prosperity at risk; countries with glass infrastructure should not throw stones. The Internet may be too fragile to indefinitely sustain the levels of nation-state attacks of recent years, and each dollar and experienced cyber professional the US government is committing to offense and espionage is one that could be used to instead improve defenses.

For billions of people, the Internet establishes a very personal, even intimate, connection. A nation that controls so much of the hardware and software that makes it work can ill afford to be cast as the villain by, frankly, seeming so villainous.

Silicon Valley, and American ICT companies more generally, is the nation's true cyber power. Yet, by coercing American technology companies to allow backdoors and other tools of espionage, US policy has imperiled this gem of US innovation. As Shane Harris puts it, "Foreign companies now view American technology, once the gold standard for performance and innovation, as tools of American spying."[37]

In the wake of revelations about the scope of US online espionage, including those that implicated American IT companies, some commentators have felt "everyone does it" and that any reduction in these operations would be "unilateral disarmament," as the United States' adversaries are still using these capabilities.[38] This mindset sees "cyber" as a zero-sum game between nations or adversaries, as if attack and exploitation were separate from US Internet policies. It promotes the undoubted national security gains of attack and exploitation as the premier goal, as if an aggressive stance will have no important blowback against the present and future gains of the Internet or the digital economy, society, and a digital future.

By way of comparison, the United States became seriously overcommitted in Vietnam in the 1960s because of a string of decisions, each of which might have made narrow national security sense at the time. Yet, the cumulative effect was a major strategic setback after a deeply divisive war, in which the country had little chance of prevailing. A similar cautionary tale could be told of the Iraq invasion of 2003.

Just so, even if each of the separate decisions for additional military cyber capabilities and online espionage operations were in the US national security interest, the sum total of them clearly is not.

5. Overestimation of the Effectiveness of Public-Sector Action: Even as technology has helped create a world in which "states pull fewer levers," the US government has, for the past decade, put the focus of its efforts on improving the government's own cyber capabilities: building new organizations, hiring more people, and instituting new programs.[39]

As it turns out, very few significant cyber conflicts, or problems of any sort, have ever been decisively resolved by governments. Instead, the decisive actions have been taken by the private sector, with its agility, subject-matter expertise, and ability to create and bend cyberspace (by adding or changing their networks). Governments lack these strengths, but do have deep pockets, endurance, and access to other levers of power.

The original model of the Internet had the government in the background while the private sector took the lead—a model successful in almost all of the Internet's early crises, such as the Cuckoo's Egg (1986) and Morris worm (1988). After the Morris worm, the US government combined the best of the private and public sectors by using Pentagon money to establish the Computer Emergency Response Center at Carnegie Mellon University, to prepare for Internet disruptions and coordinate once they hit.

The model of nonstate actors in the lead continued all the way up to the attacks against Estonia (2007) and the battle against the Conficker malware (2009).

Over time, this model was lost. Instead, the United States put government at the center, such as the creation of the US CERT and trying to make the Department of Homeland Security the prime mover for cyber defense. Government organizations do not often have the needed agility or subject-matter expertise, and lack any direct levers to affect changes at the technical layers of cyberspace.

6. The Internet Remains Offense-Dominant, with a Potentially Inevitable Tipping Point: Cybersecurity is stuck, and probably even moving backward.

As noted previously, for more than thirty-five years, the offense has had an easier time than the defense. Worse, this mismatch is not just longstanding, but getting worse. Every time there is a new technology fixing some problem or other, the attackers have found ways to improve their advantage.

Jeff Moss, creator of the DEF CON and Black Hat conferences and who wrote the foreword for this paper, believes the advantage is growing significantly worse as "[t]he balance has swung radically in favor of offense, and defense seems futile to some right now."[40] The Index of Cyber Security, which canvasses security professionals for their degree of perceived risk (similar to measuring the strength of the economy through confidence of consumer or purchasing managers), has increased every single month for more than three and a half years, more than doubling along the way.[41]

The relationship between cyber offense and defense does not have to be frozen in this dynamic; in fact, it would be odd if it never changed. In almost every other form of human conflict (except nuclear and, perhaps, space warfare), the advantage repeatedly switches between attackers and defenders. For decades, one set of practices and technology (such as the machine gun) gives one side the advantage until another set comes along (like the combination of the tank, airplane, and radio, with the doctrine to use them together).

The first implication is that US cybersecurity policy is failing badly. As Dan Geer puts it, even though cyber defenses are obviously improving, they are not keeping pace with the attackers: "Whether in detection, control, or prevention, we are notching personal bests, but all the while the opposition is setting world records." Cybersecurity experts are perennially the losing team, and have been losing since nearly the first game of the first season.

The career of every cybersecurity expert, every hour of time invested, every dollar spent—and every cyber strategy—has been, at best, only breaking even. The Comprehensive National Cybersecurity Initiative invested $40 billion over five years, yet failed to change this underlying dynamic, even though some government organizations are better protected. This suggests the need for a completely new approach.

The second implication is that, perhaps, this trend might get far worse before it gets better. Can the Internet itself survive another thirty-five years of offense advantage?

After all, for how long can a system stay in balance when one side has had a persistent advantage, year after year and decade after decade? There may soon be a tipping point, a discontinuity where there are more predators than prey. Attackers would not just have the advantage, but dominance (O>>D)—a situation recent reports by the World Economic Forum and Atlantic Council called a "Cybergeddon" or "Clockwork Orange Internet."[42] The Internet would no longer be merely the Wild West, but a failed state like Somalia, with vast implications for the global digitized economy.

7. An Unpreparedness for Global Cyber Shocks: Cyber "shocks" are likely, and there is little governance or preparation for them.

A threat to the Internet increasingly means a threat to everything. Every part of the world's societies and economies uses the same underlying infrastructure, the same hardware, software, and standards, with billions of devices connected to the Internet, from simple e-book readers to electrical-distribution networks.

The Internet of tomorrow is likely to both amplify and be a source of global shocks. The main concern is a failure of multiple local elements that leads to cascading global disruptions. The result is that organizations will suffer ever more frequent shocks that, in their nature, are like natural disasters: too severe and frequent to ever be able to sufficiently protect against.

For example, imagine if a major cloud-service provider or IT company suffered a "Lehman moment," with everyone's data there on Friday and gone on Monday. In 2014 or 2015, it was perhaps just possible to determine which dominos would hit which others in the resulting cascade. But in another two, or five, or ten years, it will be truly unknowable.[43]

Moreover, there are only organizations to respond *technically* (such as the Internet Corporation for Assigned Name and Numbers, or ICANN) and few or none that might contain a true global geopolitical and macroeconomic shock. When the financial sector (besides the Internet, the only other truly global infrastructure prone to shocks) crashed in 2008, existing groups were already in place: the Bank for International Settlements, the International Monetary Fund, the Group of Eight (G8) group of major economies, and central bankers. The Internet lacks anything similar to these mechanisms to coordinate the response to a true global cyber shock, one severe enough to demand coordination between heads of governments.

Cyber Strategy: Ends, Ways, and Means

Nearly every other long-term priority for the United States relies on having a safe and secure Internet, as a foundation for the economy and for projecting military power.

Ends

Finding a strategic and sustainable balance for US cyber interests must be accordingly built around three key ends, in order of priority:

1. **Secure Cyberspace as a Means to Advance Prosperity**: First and foremost, US policy must ensure cyberspace and the Internet advance US and global prosperity, not least through continuous and accelerating innovation. Other priorities are important, but subordinate.

National security does not mean just keeping the nation safe from terrorists or other adversaries abroad, but includes economic security as well. Being hawkish for America's long-term economic security through a resilient, sustainable Internet means being strong on national security.

The Internet is simply too critical to the proper functioning of the global economy, and should only become more so over the coming years, decades, and centuries. The United States will be strong if the Internet is strong, for the continuation of Internet-driven innovation, gross domestic product (GDP) growth, productivity improvements, and job creation.

Already, it is possible that barely restrained US cyber espionage may have fatally undermined the chances of a US-EU trade pact by infuriating German and other European allies, potentially putting 750,000 new trade-related jobs at risk.[44]

2. **Maintain an Open Internet to Support the Free Flow of Ideas**: The United States must be seen as the steward for a sustainable global Internet.

Protecting cyberspace "not only serves the material interest of the United States and its allies, but also underscores America's commitment to acting in the best interest of humankind," as emphasized in *Dynamic Stability*.[45]

Cyberspace and the Internet are American inventions, reflecting American values, and are used in all nations and by all generations. American policy should cherish this opportunity for soft power and be delicate with actions that would squander this astounding once-in-a-millennium national advantage.

"The Internet creates its own constituency," according to one US cyber diplomat.[46] No other powers can match the American promise of a free, stable, and secure global Internet. The Chinese and Russian models allow somewhat free commerce, but are optimized for internal monitoring and control, while India is not an Internet power. Europe is still too split between national governments, languages, and markets. Only the United States is positioned to be a global leader for an Internet that is at least as free and resilient for future generations, supporting the free flow of ideas and information.

Just as jazz and rock music gave form to the ideas of American freedoms and liberties, encouraging oppressed peoples on the other side of the Iron Curtain, so should an open and free cyberspace be a beacon for those in China, Cuba, and other nations.

3. Secure US National Security in and Through Cyberspace: Of course, the US military and intelligence agencies must use new technologies as well, not least because the world is becoming more dangerous and unpredictable. The president must continue to have options for computer-enabled espionage and to achieve national security objectives, including offensive cyber capabilities when appropriate and necessary (while keeping in mind that other governments also want to expand their leaderships' range of capabilities).

The concept is to have a strategic and sustainable balance to encourage cyber capabilities for espionage and attack, but with extreme caution when they conflict with other objectives, especially the United States' long-term, Internet-fueled prosperity.

These are objectives that represent the United States at its best and provide the best opportunities to leverage American strengths.

Ways

To execute a strategy built toward these three ends, the United States should pursue two overlapping approaches: making the Internet **defense dominant**, so the Internet's defenders have the advantage; and adding a time component to security concerns by aiming for a **sustainable cyberspace**. Together, these goals define the large-scale vision that should drive US strategy.

- **Defense Dominant**: It is in the long-term interests of the United States and other like-minded nations to flip the historic dynamic, so that defenders have the easier time instead of the attackers. Such a future protects US commerce and freedom of speech, while still granting the most capable attackers, the US military, options to use cyber capabilities to supplement or replace kinetic firepower.

It *must* remain imaginable to make botnets or massive denial-of-service attacks a thing of the past, like the chicken pox or polio. It *cannot* be impossible to make it so hard to spy or attack online that most sites are effectively invulnerable to all but the most dedicated of attackers. *Why cannot* the community make progress on common goals, similar to those of Kyoto or other environmental treaties, such as reducing the number of records stolen in data breach to 2010 levels by 2020?

This will require tradeoffs. As an example of what this means in practice, one of the most powerful statements on the topic is from Estonian President Toomas Ilves, who stresses that the ability to securely communicate is so critical to the modern economy and society that governments must have "no backdoors…no matter the cost" to law enforcement or espionage.[47]

- **Be Sustainable for Future Generations**: Cyberspace and the Internet are resources like any other; they can be squandered and spoiled. Even though they are not a natural resource—like the air, land, sea, or space—they can be ruined beyond use by careless actions. In fact, as their foundation is not natural, but essentially built on human trust, cyberspace and the Internet may be far more sensitive to long-term pollution and disruption.

  US policy must, accordingly, ensure that they are at least as resilient, open, and awesome for future generations as they have been for the generation of its pioneers. These fundamentals must be threaded throughout US strategies and policies. Stakeholders may need to move beyond the traditional solutions, with fresher ideas that can scale and shift away from a national security mindset. The new awareness of the health of the planet can be directly applied to the "environment" of cyberspace, polluted by viruses, malware, spam, and botnet attacks.

Means

The road to these ends and goals begins with the right strategy, which in essence is using available means to achieve foremost ends.

The most effective strategies are simple. They consist of only a few words and generate their own ideas, allowing those who follow the strategy to discover ways to apply it to new and existing problems. To defeat insurgents, General David Petraeus pursued a "population-centric" approach; win the hearts and minds of the people. In any situation, the general and his staff had a guiding principle to illuminate their strategic choices.

The only way to achieve a sustainable, defense-dominant Internet that advances prosperity is through a similarly concise approach, which includes seven key means, as follows:

1. **Issue a New Strategy Prioritizing a Defense-Dominated Cyberspace**: The single most important recommendation of this report is for the White House to issue a single, overarching national cyber strategy to balance competing priorities, built around making defense easier than offense through a nonstate-centric approach. It is far too cumbersome to balance priorities and create a common set of goals with the current approach of separate strategies to cover innovation, national security, intelligence, or Internet freedom.

For too long, US policy has tried to pursue a balance between cyber offense for America's spies, soldiers, and police, and cyber defense for everyone else. Unfortunately, pursing a "balance" means that every new case must be treated on its own merit, with no guidance from even well-meaning bureaucrats on the president's intent. Cyberspace is too complex (and likely fragile) to survive policymakers trying to walk the tightrope of keeping offense and defense in balance.

This is particularly true as the Internet of Things pervades all aspects of life and society. What would it mean for national security to strategically undermine the resilience of US hospitals, in order to preserve the possibility of espionage against another state? Which US allies would buy IoT devices for use in their offices, homes, and cars, when that equipment is likely to be used for US (or other nation-state) surveillance? What is the economic impact to the US economy from eliminating more than ninety percent of the potential global market? On the other hand, consider the economic benefit from actively pursuing a model of increased resilience and trust in US consumer goods.

The White House should, accordingly, no longer feature "balance," but take a clear, public policy stand that whenever there is a tradeoff between offense and defense, the defense should win, unless there are compelling reasons otherwise. Officials should be held accountable for meeting that priority and punished when they work against it, unless approved by the NSC.

This strategy should, for the reasons outlined in this paper, emphasize that solutions to get defense superior to offense will come overwhelmingly from the world's true cyber superpower, the US private sector—not just ICT companies, but all nonstate actors, including individuals, industry associations, volunteer groups, universities, and others—which invents, installs, and maintains these technologies. Of course, governments have a supporting role, especially with their immense resources, endurance, and access to other levers of power.

To put this in more familiar terms, when Americans think of the nation's airpower, the United States Air Force comes to mind, just as the Navy is the natural center of US maritime power. But this has not always been the case. In the 1920s, US air power was led, in no small measure, by the private sector, as aviators barnstormed and raced, pushing engineers to develop ever better technologies. It was likewise not that many decades ago when the pride of maritime power might have been not the US Navy, but the civilian Merchant Marine, which carried the nation's massive agricultural and industrial output around the globe in US-flagged ships.

Headquarters of the NSA at Fort Meade, Maryland. *Photo credit: National Security Agency/Wikimedia*

In cyberspace, the situation is even more stark, in that the true cyber capacity of the United States is largely in the private sector. Yet, the US government has not yet realized this, remaining stuck in the mistaken belief that US cyber power is centered in Fort Meade, Maryland, home of the National Security Agency and US Cyber Command.

America's true cyber power, however, is not the ability to destroy and spy, but to create and innovate. This power is not at Fort Meade, but in Silicon Valley. It is not on Route 32 in Maryland, but Route 128 in Massachusetts, and countless other office parks (and basements) around the nation.

Few, if any, major Internet crises have ever been decisively resolved by any government anywhere. Rather, nonstate actors have been most critical. A successful cyber strategy must, therefore, accept this central role of the private sector and then work outward from that core US strength. Wherever possible, solutions to governance, regulation, protection, and response must stem from this core.

As argued in *Dynamic Stability*, the first *Atlantic Council Strategy Paper*, US leaders must become more comfortable playing a multilevel game, working with nonstate actors "who possess a greater range of capabilities than at any time in history."[48] A nonstate-centric approach does not mean the government must surrender to nonstate actors. The best solutions will reinforce the strengths of both states and nonstate actors.

Best of all, such a strategy fits in perfectly with the "third offset" of the Department of Defense, which seeks new innovations that preferentially advantage the United States over adversaries who are rapidly closing the gap in military capabilities. Neither Russia nor China—and certainly not Iran or North Korea—can match the dynamic power of the US private sector.

Often, government officials or military officers dismiss the private sector. After all, cyber problems would be far less severe if companies properly secured their systems or made more secure software. It is true that many companies fail to take these kinds of common-sense steps, but this mindset is a strawman that oversimplifies cyber problems and the category of nonstate actors. This fallacy will be discussed in the next sections.

2. Improve US Government Processes on Cyber: While working on that strategy, the White House should **reinvigorate the interagency cyber process** to include more outside voices, especially from officials who can advocate for the overriding priority of prosperity, even in the face of hardcore national security practitioners. This could be done by widening the current National Security Council (NSC) interagency process, splitting out the previous Homeland Security Council to have a more balanced domestic focus, or balancing the NSC interagency process with the parallel process of the National Economic Council, which is more focused on the true top priorities of innovation and prosperity.

The new process should find some more effective way to include nonstate voices and advice in the process. Currently, groups like the National Security Telecommunications Advisory Committee have a purely advisory role, making them easy for busy White House staffers and DHS bureaucrats to ignore. Multi-stakeholder governance is something the US government supports for the Internet as a whole, but rarely for United States policymaking itself. Other nations often embed companies or technologists in governance, as is the case in the Netherlands, whose Cyber Security Board includes key Dutch companies. Perhaps the only way for the US government to approach this kind of bold step is to build a private-sector-led response capability, driven by major cybersecurity companies and the major telecommunications companies, as well as hardware and software vendors.

On offense and espionage, the US government has been streamlined and risk seeking, but it is meek and stumbling on defense. Therefore, it is likely time to **either fix the DHS cyber organization or split it off into a new cyber agency**, alongside the Information Assurance Division (IAD) of NSA, the National Telecommunications and Information Administration of Commerce, and other cyber and Internet organizations.

NSA's IAD is one of the few true gems of cyber defense in the US government, and the mainstream belief is that it must stay at NSA because the best way to become the best defenders in the world is to work alongside the most capable attackers. This may be true if the US government's foremost cyber goal is to use the Internet to spy and, when necessary, attack others through cyberspace; but, if the goal is instead Internet-driven prosperity, perhaps it is folly *not* to split them.

The Internet is so new and transformative (and US policymaking so tangled) that this new cyber agency could even be a US version of a European-style Ministry of Telecommunications, perhaps a Department of Information and Communication Technologies.

3. Sow the Seeds for Disruptive Change: Defenders must continue technology and process innovations to try to change the nature of the battlefield and the weapons. Unlike the air, land, sea, or space, the Internet was crafted by, and is still being shaped, by humans. The world is not bound by the physics of cyberspace in quite the same way as other domains. If people dislike some characteristics of water and the ocean, all they can do is work around them, inventing new vessels that exploit hydrodynamics in novel ways. But with cyberspace, they can invent new technologies with different characteristics—technologies that change the fundamental medium itself, not just how it is used.

Accordingly, technologists must continue to look for game-changing new technologies and processes that can, either on their own or in combination, radically improve defenses. The most obvious candidate is a new, more secure Internet with security built in from conception. However, any Internet with such characteristics may not be as global, since the Chinese and Russians would be sure to influence the standards process so that any new Internet would be more friendly to their priorities of control over freedom.

Another path to disruptive change is to prioritize solutions that scale, so that a dollar of defense buys far more than a dollar of attack. Currently, a New York Cyber Task Force, run by the School of International and Public Affairs at Columbia University, is compiling a list of past policy, operational, and technological solutions that have most allowed defenders to outpace attackers. These innovations, including encryption and the launch of Microsoft's Windows Update to easily update computers with more secure software, had one thing in common: they massively and easily scaled, so that one relatively inexpensive action protected millions or billions of computers. Other innovations have come from new operational methods or organizations, such as information sharing and analysis centers or the "cyber kill chain," while others have been policies, such as norms to try and restrain use of national offensive capabilities.

Thinking about past successes in this way should guide decisions on future disruptive solutions, such as those that could take away entire classes of attacks. The efforts of the Defense Advanced Research Projects Agency (DARPA) to revive "formal methods" for provably

Steve Weber, faculty director at the UC Berkeley Center for Long-Term Cybersecurity (CLTC) speaking at a Cybersecurity Futures 2020 event in Washington, DC, on April 28, 2016. *Photo credit: CSM Passcode/YouTube*

secure systems are one example, in which "obvious pathways for attackers…have all been shut down in a way that's mathematically proven to be unhackable for those pathways."[49] Such transformative solutions are especially needed for the Internet of Things, whose devices will far outnumber actual human users on the network. Those devices are, all too often, indefensible.

Research grants should continue to foster such innovations. A wonderful nonstate example is the recent $15 million grant by the William and Flora Hewlett Foundation to create a Center for Long-Term Cybersecurity at the University of California at Berkeley. New game-changing policies could include changing the laws on software liability so that vendors could be held responsible for faulty, insecure code that harms others as part of an attack.

The Atlantic Council's Cyber Statecraft Initiative has made security of the Internet of Things—especially those aspects such as medical devices and automobiles, which have direct impacts on life and safety—the top priority for its future work.

4. Develop Grants to Extend Nonstate Capabilities: Another idea, which comes naturally from a nonstate-centric approach, is to combine the resources of government with the agility of the private sector. This could mean for DHS and the Defense Department to provide small to medium-sized grants to key nonstate groups at the center of defense, which are already saving cyberspace every day.

The Financial Services Information Sharing and Analysis Center, or FS-ISAC, has won awards for being the best information-security organization.[50] Yet, this group was nearing capacity and potential decline when, in 2003, it received a $2 million grant from the Treasury Department to expand its management and warning capabilities and improved technology. Many other information-sharing and response groups could use a grant of this size (or even a far smaller one) to build capacity through new staff and technology.

The ShadowServer Foundation collects intelligence on cyber operations and is used extensively by the Federal Bureau of Investigation (FBI) to take down "botnet" networks of infected computers. Yet, it is a volunteer network of individuals, with only a handful of full-time staff and a budget of perhaps only $10 million. The Open Source Vulnerability Data Base, run on perhaps $10,000 a year, contains more information on vulnerabilities than the official DHS-funded National Vulnerability Database, which has millions of dollars in funding.

A program of small grants could vitalize the volunteer and other nonstate groups, achieving far more than if the same money were to be spent in DHS or at Fort Meade.

5. Regulate for Transparency, Not Security: The central "regulation" mechanism of US-style capitalism is that publicly traded companies are responsible primarily to their shareholders. So, if a publicly traded company is making terrible cyber-risk decisions, that is first and foremost an issue for shareholders, operating through their board of directors.

The Department of Homeland Security should largely cease trying to convince chief information security officers or board directors, one company at a time, to take cyber risks seriously. This same effort could be directed at convincing institutional shareholders like CALPERS or BlackRock, which can then take the issue directly to managers or pressure directors at shareholder meetings.

Likewise, the government should rarely regulate through security standards; rather, it should regulate through transparency, reinforcing existing private-sector mechanisms. The current Securities and Exchange Commission (SEC) guidance is a perfect example of being both nonstate centric and working at scale.

Rather than tell companies how to secure themselves and detailing their responsibilities in hundreds or thousands of pages, the SEC uses just four pages, barely two thousand words, to remind boards that shareholders should be informed of any "material" cyber incident. If companies ignore the advice, they leave themselves open to shareholder lawsuits.[51]

6. Long-term Focus on Systemic Risk and Resilience: Cyber problems today are mostly experienced as a series of incidents, such as one company at a time being taken down by a denial-of-service attack or intruded by hackers or an intelligence service. Yet, cyber problems might not just be a string of such incidents, but a true global shock. If one of the too-big-to-fail ICT companies had a "Lehman moment," with everyone's data there on Friday and gone on Monday, it would be experienced as a shock that could cascade out from the initially affected companies to take down the organizations that depend on them, and so on and so on.[52]

Large-scale cyber shocks are just as inevitable as natural disasters. Cyberspace has simply become too hyperconnected to try to stop or predict all the possible failure modes.

Some governments have begun to look at mitigating risks from an increasingly interconnected and coupled world, such as the US work on "complex catastrophes." However, risk management and response still focus mainly on the risk and response carried out within individual organizations, looking to prevent incidents—not on shocks.

While the Internet crisis-management community has, so far, been successful at ensuring failures do not develop into a full-scale collapse, the system will not be able to adequately address a truly global, cascading shock. The approach is largely ad hoc, centered on incident management rather than crisis response, and often staffed by poorly funded organizations or individuals who have numerous other responsibilities. To be ready for cyber shocks, Internet stakeholders must conduct exercises, develop response playbooks, and increase funding and grants (see below) for such large-scale crisis management.

7. Look Beyond a Security Mindset to Sustainability: Policies that look to the **sustainability of cyberspace** are a rich source of new solutions. "Cybersecurity" on its own has no time horizon, no easy way to make tradeoffs between today's needs and those of the future. Sustainability, wanting future generations to have an Internet that is as rich, open, and secure as the one today, is the easiest way to address these issues. It also views the Internet not as a "domain" or "global commons," but, more straightforwardly, as an *environment*.

Thinking of cyberspace as an environment creates several advantages. Environmental norms (such as "polluter pays" or "think globally, act locally") can be directly applicable to cyber risks. Such norms of protecting the common good are strongest among the youngest generation, those who are digital natives. Environmentalism also provides a much stronger role for companies, individuals, and nongovernmental organizations, compared to seeing risks as problems of crime, espionage, or warfare.

For example, pursuing a sustainable cyberspace would help integrate cybersecurity with capacity building. It might also help snap today's debate out of the unproductive deadlock of security versus privacy. Large-scale surveillance or erecting Internet borders might be seen as unsustainable practices, just as at odds with the future as clear-cutting tropical forests or emitting endless carbon dioxide. It could be a true game changer if nations could agree on a basic promise, such as "clean food, clean water, clean Internet," to bring together thinking on development and security.

All nations must pollute to some degree, so one environmental goal is to keep a low "emissions intensity" to, for example, minimize the amount of pollution per unit of GDP. Similarly, nations should aim to have the fewest infected computers per thousand computers or per unit of GDP—something that is not just measurable, but actually measured today. This kind of change in mindset could allow new solutions, such as if nations and global companies promised, using the language of the environmental movement, a pledge "to bring botnets down to their 2005 levels by 2020."

Bringing together cybersecurity researchers, cyber companies, and decision-makers to propose and enact solutions to these issues will remain a critical task for the Atlantic Council. The confluence of dependence on vulnerable, exposed cyber systems—with the rise of new actor classes willing to exploit weakness for their ends—poses systemic risks to public safety, human life, national security, and GDP. Dependence on connected technology is increasing faster than the ability to build defensive capabilities and resilience. In order to establish sustainable and survivable cyberspace, new problem spaces and solution sets must be investigated and evaluated.

Conclusion

As the world becomes increasingly tumultuous, so too will cyberspace and the Internet domain, unless the United States adopts a nonstate-centric strategy. It is up to the United States to ensure that its ideals prevail online to keep the Internet and ICT open to all, safe to use, and as awesome as before.

The United States, and all of those who use any device connected to cyberspace, should never lose sight that increased interconnectivity is the single best way to advance prosperity, democratic values, and individual empowerment around the world. Should anything come to harm the Internet or cyberspace, or even marginally increase the risk of increased connectivity, all of this potential goes away.

Government certainly has a role to play. Yet, to save cyberspace—and, thereby, the future—the public sector must learn how to leverage the private sector and other nonstate actors. A strategy that plants the fulcrum within government bureaucracies will never accomplish great defensive successes. The leverage is outside of government. This does not mean relinquishing authority, but recognizing that there are nine players on the baseball field, and a nonstate actor is usually closest to the ball and able to make the play.

This may go against many of the instincts of the Trump administration, but a defense-first strategy, based on the strengths of America's nonstate cyber defenders, is the best hope for American prosperity and security.

Endnotes

1. Future work from the Atlantic Council will dive far more deeply into the implications for economic and physical safety of an insecure Internet of Things. In particular, the Atlantic Council is focusing on "cyber safety," such as interconnected and autonomous automobiles, hospitals and medical devices, and the electric grid.

2. Barack Obama, "Remarks by the President at the Cybersecurity and Consumer Protection Summit," speech delivered at Stanford University, February 13, 2015, https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

3. Barry Pavel and Peter Engelke with Alex Ward, *Dynamic Stability: US Strategy for a World in Transition* (Washington, DC: Atlantic Council, 2015), p. 17, http://www.atlanticcouncil.org/publications/reports/dynamic-stability-us-strategy-for-a-world-in-transition.

4. Jason Healey, *Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures* (Zurich, Switzerland: Atlantic Council, Frederick S. Pardee Center for International Futures and Zurich Insurance Group, 2015), http://publications.atlanticcouncil.org/cyberrisks/.

5. Dan Geer, "We Are All Intelligence Officers Now," talk at RSA Conference, February 28, 2014, http://www.rsaconference.com/writable/presentations/file_upload/exp-f02-we-are-all-intelligence-officers-now.pdf.

6. Healey, *Overcome by Cyber Risks?*

7. Roger R. Schell, "Computer Security: The Achilles Heel of the Electronic Air Force?" *Air University Review*, January-February 1979, http://www.airpower.maxwell.af.mil/airchronicles/aureview/1979/jan-feb/schell.html.

8. Bruce Schneier, "Liability Changes Everything," *Schneier on Security* (blog), November 2003, https://www.schneier.com/essay-025.html.

9. *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: National Research Council, 1991), p. 14, https://www.nap.edu/catalog/1581/computers-at-risk-safe-computing-in-the-information-age.

10. Charles Perrow, *Normal Accidents: Living with High Risk Technologies* (Princeton, NJ: Princeton University Press, 1984), p. 85.

11. Leonid Bershidsky, "Millennials Want Apps, Not Cars," *BloombergView*, July 15, 2014, http://www.bloombergview.com/articles/2014-07-15/millennials-want-apps-not-cars.

12. For estimates on exactly how many devices, see Gartner, press release, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units by 2020," December 12, 2013, http://www.gartner.com/newsroom/id/2636073; Jason Dorrier, "Is Cisco's Forecast of 50 Billion Internet-Connected Things by 2020 Too Conservative?" *SingularityHub*, July 30, 2013, http://singularityhub.com/2013/07/30/is-ciscos-forecast-of-50-billion-Internet-connected-things-by-2020-too-conservative/.

13. Kenneth Neil Cukier and Viktor Mayer-Schoenberger, "The Rise of Big Data: How It's Changing the Way We Think About the World," *Foreign Affairs*, May/June 2013, http://www.foreignaffairs.com/articles/139104/kenneth-neil-cukier-and-viktor-mayer-schoenberger/the-rise-of-big-data.

14. Network neutrality is the idea that the Internet, by design, does not care what kind of information it is transporting, only that it arrives. Companies are exploring the idea that some kinds of information could be put in a special "fast lane," ensuring faster delivery, though at a higher price. Others disagree, suspecting that innovative new entrants would be locked out of the system, unable to pay to get their content in the fast lane.

15. Centre for International Governance Innovation and IPSOS, "2014 CIGI-Ipsos Global Survey on Internet Security and Trust," November 2014, https://www.cigionline.org/internet-survey.

16. According to a 2013 report to the UN Secretary General, and agreed to by fifteen national experts, "State sovereignty...apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory." United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," June 24, 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

17. "Virtual Counter-revolution," *Economist*, September 2, 2010, http://www.economist.com/node/16941635.

18. White House, *International Strategy for Cyberspace*, May 2011, p. 4, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

19. Federal Communications Commission, "National Broadband Plan," http://www.fcc.gov/national-broadband-plan; White House Office of Science and Technology Policy, "Technology and Innovation," http://www.whitehouse.gov/administration/eop/ostp/divisions/technology; National Institute of Standards and Technology, "National Strategy for Trusted Identities in Cyberspace," http://www.nist.gov/nstic/.

20. Secretary John Kerry, "An Open and Secure Internet: We Must Have Both," remarks at Korea University in Seoul, May 18, 2015, http://www.state.gov/secretary/remarks/2015/05/242553.htm.

21. Ibid.

22. Ibid.

23. US Department of Justice, "Cyber Crime," http://www.justice.gov/usao/briefing_room/cc/.

24. James B. Comey, "Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy, Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee," July 8, 2015, https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.

25. Harold Abelsen, Ross Anderson, et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications," *DSpace@MIT* (blog), July 6, 2015, https://dspace.mit.edu/handle/1721.1/97690.

26. US Department of Defense, *DoD Strategy for Operating in Cyberspace*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf .

27. *DoD Cyber Strategy*, April 2015, pp. 4-5.

28. For a book-length examination of these incidents, see Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014).

29. Ryan J. Reilly and Matt Sledge, "FBI Director Calls On Congress to 'Fix' Phone Encryption by Apple, Google," *Huffington Post*, October 16, 2014, http://www.huffingtonpost.com/2014/10/16/james-comey-phone-encryption_n_5996808.html.

30. Aliya Sternstein, "Justice is Fast-Tracking Cyber Hires," *NextGov*, May 15, 2014, http://www.nextgov.com/cybersecurity/2014/05/justice-fast-tracking-cyber-hires/84511/.

31. US Senate Armed Services Committee, "Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander," March 11, 2014, http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf.

32. Center for Strategic and International Studies, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization" (Washington, DC: CSIS, 2011), http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

33. Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics*, vol. 30, no. 2, January 1978, pp. 167-214, http://www.jstor.org/stable/2009958?seq=1-%20page_scan_tab_contents#page_scan_tab_contents.

34. Quote taken from Ralph Langner, "The Equilibrium of Cyber Conflict: In Memoriam John Nash (1928-2015)," *Langer.com* (blog), May 24, 2015, http://www.langner.com/en/2015/05/24/the-equilibrium-of-cyber-conflict-in-memoriam-john-nash-1928-2015/.

35. *International Strategy for Cyberspace*, opening statement by President Obama.

36. It has been reported in the media—and widely believed by computer scientists—that NSA put a backdoor in a new cryptographic security standard, called Dual_EC. See Bruce Schneier, "Did NSA Put a Secret Backdoor in New Encryption Standard," *Wired,* November 15, 2007, http://www.wired.com/2007/11/securitymatters-1115/. To better get spying software into Iranian computers, to gain intelligence for the later Stuxnet attack, it appears the US government (most likely NSA) conducted an attack to subvert Windows Update on select Iranian computers. This attack subsequently appeared in the wild and caused a significant emergency response effort within Microsoft. Ellen Nakashima, Greg Miller, and Julie Tate, "U.S. Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *Washington Post,* June 19, 2012, https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html; John Leyden, "Crypto Collision Used to Hijack Windows Update Goes Mainstream," *Register,* November 5, 2014, http://www.theregister.co.uk/2014/11/05/md5_hash_collision/.

37. Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York: Mariner Books, 2014), p. 227.

38. Bruce Schneier, "There's No Real Difference Between Online Espionage and Online Attack," *Atlantic,* March 6, 2014, http://www.theatlantic.com/technology/archive/2014/03/theres-no-real-difference-between-online-espionage-and-online-attack/284233; David E. Sanger, "White House Details Thinking on Cybersecurity Flaws," *New York Times*, April 28, 2014, http://www.nytimes.com/2014/04/29/us/white-house-details-thinking-on-cybersecurity-gaps.html?_r=0.

39. Pavel and Engelke, *Dynamic Stability*, p. 8.

40. Jeff Moss, aka "The Dark Tangent," introduction to program guide for DEF CON 21 conference, 2013.

41. Index of Cyber Security, "ICS Value, September 2016=3406," http://www.cybersecurityindex.org/.

42. World Economic Forum, *Global Risks 2013: Eighth Edition* (Geneva, Switzerland: World Economic Forum, 2013), http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf; Healey, *Overcome by Cyber Risks?*

43. For more on a "Lehman moment," "cyber subprime," and related ideas on cyber shocks, see Jason Healey, "Beyond Data Breaches: Global Interconnections of Cyber Risk" (Zurich, Switzerland: Atlantic Council and Zurich Insurance Group, 2014), http://www.atlanticcouncil.org/publications/reports/beyond-data-breaches-global-interconnections-of-cyber-risk.

44. Atlantic Council, "TTIP and the Fifty States: Jobs and Growth from Coast to Coast" (Washington, DC: Atlantic Council, 2013), http://www.atlanticcouncil.org/images/publications/TTIP_and_the_50_States_WEB.pdf.

45. Pavel and Engelke with Alex Ward, *Dynamic Stability*, p. 33.

46. Daniel Sepulveda, comments at Columbia University SIPA, Global Digital Futures Policy Forum, April 25, 2016.

47. Toomas Ilves, comments to Columbia University SIPA conference on Digital Development and Technology, April 13, 2016.

48. Pavel and Engelke with Alex Ward, *Dynamic Stability*, p. 17.

49. Kelsey D. Atherton, "How DARPA is Prepping for the Next Cyberwar," *Popular Science*, February 11, 2016, http://www.popsci.com/darpa-is-building-tools-for-next-cyberwar.

50. FS-ISAC, press release, "FS-ISAC Receives 2013 Award for Excellence in Information Security," February 26, 2013, https://www.fsisac.com/sites/default/files/news/FS-ISAC-Receives-RSA-Award.pdf.

51. US Securities and Exchange Commission, "CF Disclosure Guidance: Topic No. 2: Cybersecurity," October 13, 2011, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

52. For more on the themes in this section, see Healey, "Beyond Data Breaches."

About the Author

Jason Healey is senior research scholar at Columbia University's School for International and Public Affairs, specializing in cyber conflict and risk. He started his career as a US Air Force intelligence officer, before moving to cyber response and policy jobs at the White House and Goldman Sachs. He was founding director for cyber issues at the Atlantic Council where he remains a senior fellow and is the editor of the first history of conflict in cyberspace, *A Fierce Domain: Cyber Conflict, 1986 to 2012*. He is on the DEF CON review board and the Defense Science Board task force on cyber deterrence.

Acknowledgments

The author would like to acknowledge the team at the Brent Scowcroft Center on International Security who helped on this report and have kept the Atlantic Council at the forefront of strategic issues. In addition, the support and encouragement of the School of International and Public Affairs at Columbia University has been instrumental.

Atlantic Council Board of Directors

"The underlying Internet we depend on for our social, cultural, economic, and individual empowerment is nowhere near secure enough to hold what we are building on top of it. For these reasons, this Atlantic Council Strategy Paper that Jason Healey offers, "A Nonstate Strategy for Saving Cyberspace," is important."

– Jeff Moss

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1030 15th Street, NW, 12th Floor, Washington, DC 20005
(202) 463-7226, www.AtlanticCouncil.org