THE CYBER SECURITY PROJECT

Too Connected To Fail

How Attackers Can Disrupt the Global Internet, Why It Matters, And What We Can Do About It

Charley Snyder

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
MAY 2017

The Cyber Security Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Statements and views expressed in this report are solely those of the authors and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Design & Layout by Andrew Facini

Copyright 2017, President and Fellows of Harvard College
Printed in the United States of America

THE CYBER SECURITY PROJECT

Too Connected To Fail

How Attackers Can Disrupt the Global Internet, Why It Matters, And What We Can Do About It

Charley Snyder

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
MAY 2017

About the Author

Charley Snyder is an Affiliate of the Belfer Center's Cyber Security Project. Charley recently concluded several years of service in the Office of the Secretary of Defense (OSD), U.S. Department of Defense. Most recently he was Deputy Director of Strategic Cyber Defense and Capabilities, where he developed strategy and policies to counter foreign cyber threats and protect U.S. networks. Charley also focused on modernizing the Department's information security technologies, culture and processes, and built the Hack the Pentagon Bug Bounty Pilot and the Department of Defense Vulnerability Disclosure Program. Previously, he served as professional staff member in the U.S. Congress working on cybersecurity and counterterrorism issues. Charley has a B.S. from Cornell University and an M.A. in Security Studies from Georgetown University. He is a recipient of the OSD Medal for Exceptional Civilian Service and was a SANS Institute Difference Maker in 2016.

Acknowledgements

The author would like to thank **Gary Belvin**, **Kate Bjelde**, **Ben Buchanan**, **Dan Guido**, **Danny McPherson**, **Stuart Russell** and **Michael Sulmeyer** for their insights on earlier drafts of this paper. Any errors are the author's alone.

Table of Contents

Introduction 1

Core Internet Infrastructure and Interdependencies in Modern Society 5

Threats to Core Internet Infrastructure and Services 9

- Border Gateway Protocol Hijacking 9
- Certificate Authority Compromise 10
- Threats to cables 12
- Domain Name System threats 12

Nation State Intentions and Capabilities 17

- Suspected Attacks 18
- National Internets as Walled Gardens 21
- Use in a Conflict 23

Safeguarding the U.S. from Threats to Core Internet Infrastructure: Recommendations 27

- Raise Awareness 28
- Spur the Development and Adoption of Technical Solutions 30
- The Internet as Critical Infrastructure 30
- Build Resiliency 32
- Norms 33

Conclusion 34

Notes 36

Introduction

In March of 2015, China turned the backbone infrastructure of its domestic internet—providing connectivity to roughly 700 million people—into a weapon. Using a tool dubbed the Great Cannon, it launched an assault on the networks of a United States company called Github, which was providing safe harbor for content deemed objectionable by the Chinese government. It did so by redirecting internet traffic heading into China towards Github's offending websites, taking the company off-line by swamping it with traffic.[1]

Nine months later, the reverse happened to Turkey. In December 2015, their domestic internet became a target. Still unidentified attackers flooded Turkey's top-level domain name servers with traffic, effectively severing access to all 400,000 web sites and services (including email) using Turkey's .tr country code.[2] Here, attackers were not targeting Turkey's banks, social networks, or its government. They were attacking everything because they were attacking connectivity itself.

These cases illustrate three central points: the infrastructure that powers global connectivity can be manipulated and attacked; these kinds of attacks can be used to achieve strategic, geopolitical aims; and when connectivity fails, services relying on connectivity fail too. In the rush to reap the benefits of technology, societies have created interconnected systems that link internet infrastructure, physical critical infrastructure, and other networks with businesses and users across the globe. These networks are too complex to accurately map, let alone effectively manage. In this era, attacking the connectivity binding all these devices and systems together will become an increasingly attractive technique for nation states seeking to achieve their goals, and the most open, networked countries will be the most vulnerable. Governments that fail to account for this development– ones that invest inordinate resources to protect government networks and critical infrastructure like power and water without adequately addressing

1 Bill Marczak and Nicholas Weaver et al, 'China's Great Cannon,' Citizen Lab, 10 April 2015.

2 Efe Kerem Sozeri, 'Turkish Internet hit with massive DDoS attack,' The Daily Dot, 17 December 2015.

the connectivity that underwrites the entire system – do so at considerable risk.

* * *

Most users take the internet for granted. It is seamlessly woven into our lives, just as important for social life as it is for business. That we always expect connectivity, despite the occasional lapse on an underground subway car or on an elevator, is a testament to its resilient design.

Lately, however, many users have learned that the internet is not one amorphous "thing"—it is an extremely complex bundle of technologies that, while resilient, relies on a key set of widely deployed hardware, software, and protocols. When the security of any of these components is compromised, the security of the internet itself may be affected. When these components fail entirely, so goes the internet. These components are "too connected to fail."

This February, an incident at Amazon Web Services' popular cloud storage service, serving approximately 40% of the public cloud market, rendered thousands of websites that were hosted by the service unavailable for half a day.[3] A few days prior, a serious vulnerability was discovered at the content delivery company CloudFlare. The company, unknown to average users, serves as much as 10% of global internet traffic on a daily basis, and the vulnerability potentially compromised security for the users of as many as six million websites.[4] But these incidents were not nearly as newsworthy as an attack in October 2016 on an obscure internet company, Dyn, disrupting a key internet protocol: the domain name service. This attack rendered Twitter, Netflix, Reddit, and a host of other popular websites and services inaccessible to users in the U.S. and Europe for most of a day. It was billed as an attack on the internet itself, and was particularly noteworthy because it was launched by thousands of compromised consumer devices such as webcams and digital video recorders.[5]

3 Nick Wingfield, 'Miscue Calls Attention to Amazon's Dominance in Cloud Computing,' The New York Times, 12 March 2017.

4 Thomas Fox-Brewster, 'How Bad Was Cloudbleed? 1.2 Million Leaks Bad,' Forbes, 1 March 2017.

5 David E. Sanger and Nicole Perlroth, 'A New Era of Internet Attacks Powered by Everyday Devices,' The New York Times, 22 October 2016.

But in tightly connected societies, far more than Netflix and Twitter can be impacted when the internet is disrupted. Many critical infrastructure networks across the United States rely directly or indirectly on global routing connectivity, and attacks on core internet infrastructure can cause collateral disruptions to banking, energy, emergency services, and other societal functions. Worse, the full scale of interdependency between various critical infrastructure networks and the internet is poorly understood. These are not theoretical risks. The internet backbones of entire nations have been attacked in places like Turkey and Estonia, with impacts on various critical infrastructure sectors.

What kind of adversary might chance an attack with such broad and high-collateral effects? Perhaps those who have walled off their own domestic internet from the rest of the world. Russia, China, and Iran have all invested in the ability to separate their domestic internet from the vagaries of the global internet commons.[6] While the justification for this isolation is often to shield their citizens from harmful content–and Western spies–such a step has the added benefit of making them less susceptible to attacks from abroad that target core internet services. Indeed, these nations have demonstrated the intent and capability to conduct attacks against these very services to achieve geopolitical goals at the expense of their adversaries.

This paper will examine attacks on core internet infrastructure through a lens of national security and nation state conflict. To date, much of the discussion surrounding the recent attacks at Dyn and elsewhere have focused on consumer and economic issues. The explosive rise of poorly-protected Internet-of-Things (IoT) devices and their use in botnet attacks like the one targeting Dyn have fueled conversations about device security, regulation, and software liability. Most analyses have focused on the ability of non-state actors to use these tools to exact ransom or commit mischief. While these are real concerns, an examination of these attacks' applicability in nation state conflict has been missing.

6 Cory Bennett, 'China, Russia seeking their own Internet, warns former Intel chairman,' The Hill, 12 May 2015.

Likewise, conversation about nation state cyber conflict in national security circles seldom focuses on these types of attacks. Discussion about information security threats in the national security community often focuses on high-end destructive attack scenarios against traditional critical infrastructure and military systems. U.S. executive branch and congressional leaders often hyperventilate about a "cyber Pearl Harbor," usually referring to malware that destroys the power grid or other life-sustaining critical infrastructure. In military circles, planners worry about vulnerabilities in major weapons systems and platforms such as the F-35 that would provide adversaries an asymmetric advantage in a conflict. While destructive attacks must be accounted for, attacks on internet infrastructure are cheaper, easier to execute, and may have a broad impact across key sectors–which could make these attacks an enticing first step in an escalating conflict. As a nation dedicated to an open internet policy with a society deeply dependent on connectivity, the United States is particularly vulnerable to these attacks.

This paper argues that threats to core internet infrastructure and services can, in fact, rise to the level of a serious national security threat to the United States and will explore scenarios where this may be the case. The paper will discuss several kinds of core internet services and infrastructure and explore the challenges with understanding interdependencies between the internet and critical infrastructure; review recent attack techniques that can cause systemic risk to the internet; discuss various nation state capabilities, intentions and recent activities in this area; and describe how these attacks could be used against the United States to deter the U.S., control escalation, or potentially degrade U.S. warfighting capabilities in a conflict. Finally, the paper concludes with recommendations for what the United States and other governments can do to build defenses and resiliency against systemic threats to the internet.

Core Internet Infrastructure and Interdependencies in Modern Society

The internet is distributed and decentralized by design. Started as a Defense Department research project called 'ARPANet', its goal was to foster resilient and survivable communications (whether the specific goal was to survive nuclear attack is a controversy that remains to this day). Voice and data communications until that time relied on circuit switching—where each communication had a dedicated, end-to-end circuit connection. The ARPANet relied on packet switching technology, with the result that data could be routed in multiple paths, skirting around any outages. That technology forms the core of what we now call the internet.

The internet today is a massively distributed network of networks spread across the globe, buried under the ground and at the bottom of the ocean, laced across our cities and towns, and flying through space. It consists of a tangled web of hardware, software, and communication protocols. The hardware includes the servers that present, process, store, and route information, the fiber optic wiring that links nodes together, and, of course, the end-user devices patched in through internet service providers. The software includes programs and services to enable users to access content, communicate securely, and administer networks. Protocols tie the software and hardware together and provide a common language so that, for example, a user with an iPhone in Kenya can access web content hosted on a Linux server in the Netherlands that was uploaded by a user with a Dell laptop running Windows in Alabama. Together, these components comprise the internet.

Some of these components are more critical to its functioning than others. A number of key services are distributed through the entire internet ecosystem. Without them, the internet as we know it would cease to function. For example, the availability of the internet–the ability for users to access a resource–depends on services that can find where that resource is located and provide instructions to route requests from one location to another. Without the hardware, software, and protocols that provided these

services, the internet would no longer be available to users. Likewise, the confidentiality and integrity of data on the internet–the ability for users to access and use resources without their data being read or manipulated by unauthorized entities—relies on hardware, software, and protocols that encrypt data and ensure that users are properly authenticated. Without these services, there would be no trust on the internet, and it would cease to be an engine for the global economy. Threats to these core infrastructure and services are the subject of this paper.

While the internet's future is important on its face, it is all the more crucial given the complex interdependencies that abound between the internet and critical infrastructure. Some critical infrastructure sectors rely on the internet more than others, but all sectors are touched by it in one form or another. Many critical infrastructure networks communicate via virtual private networks, where traffic travels through an encrypted tunnel over commercial fiber wiring. While this protects the confidentiality and integrity of the data, its availability is still reliant on public internet routing that can be disrupted. Even systems that are logically separated from the internet may share power, cooling, or hardware components, and risks to one will spill over to the other. In 2014, researchers working with Shodan, a web-based tool that enumerates devices connected to the internet, found that over half a million U.S.-based industrial control devices, including programmable logic controllers and remote terminal units that give instructions to physical infrastructure such as generators and air conditioning systems, were directly accessible from the internet.[7] A recent TrendMicro report, focusing on connectivity in U.S. cities, used Shodan records to identify tens of thousands of systems belonging to city governments, emergency services, and public utilities.[8] Many of these connections may be intentional, albeit risky—for example, industrial technicians may set up a connection to remotely monitor systems for convenience and efficiency. But many more are the result of misconfigured devices that should never have been connected to the internet.

Interdependencies between critical and non-critical networks are poorly understood and the full extent of network relationships is often unclear until something goes wrong. For example, beginning a few days after the

7 'Project SHINE (Shodan Intelligence Extraction): Findings Report,' Infracritical, 1 October 2014.

8 Numaan Huq, Stephen Hilt, and Natasha Hellberg, 'US Cities Exposed: Industries and ICS,' TrendMicro, 15 February 2017.

terrorist attacks of September 11, 2001, disruptions at the New York Internet Exchange Point, a major site where large internet service providers exchange internet traffic, led to widespread internet outages in the U.S. and abroad. This was not due to any damage done to the specific exchange point. Rather, the building hosting the internet exchange lost power after the attacks and switched to back-up power generators. The poor air quality in Manhattan in the aftermath of the attacks impeded cooling at the data centers, causing the generators fueling the exchange point to consume more fuel. After two days, the fuel for the generators ran out.[9] Fuel trucks could not supply the site because vehicle traffic into Manhattan was restricted to first responders. For two days the site lost power until additional fuel could be secured, causing major internet disruptions. This is an example of the cascading failures that can result from interdependencies between different critical infrastructure systems. That particular example demonstrates how a disruption in other critical sectors (power and energy) can lead to internet disruptions, but the reverse can be true as well: if the internet disrupts the operations in one key sector, this disruption can cascade to create effects in another.

This deep interdependency powers our economy and is integral to modern life, but it comes with downsides. Threats from determined adversaries are not theoretical. In late 2016, unknown attackers conducted a distributed denial of service (DDoS) attack on the heating systems in at least two apartment buildings in Finland, causing heating to fail in the middle of winter.[10] The control systems were likely connected to the internet so they could be remotely monitored and administered, but this attack demonstrates the serious risk such connection causes. More recently, people who used connected thermostats to control their heating found them unusable due to the Amazon Web Services outage mentioned in the introduction.[11] As this paper will demonstrate, attacks against the internet can have far broader consequences than these specific examples, and can be used as a coercive tool in nation state conflict.

9 Rich Miller, 'Challenging Week at 25 Broadway: Telehouse facility wrestles with generator outages, fuel shortages,' CarrierHotels.com, 17 September 2001.

10 'DDoS attack halts heating in Finland amidst winter,' Metropolitan.fi, 7 November 2016.

11 Darrell Etherington, 'Amazon AWS S3 outage is breaking things for a lot of websites and apps,' TechCrunch, 28 February 2017.

These dependencies are just as present in the U.S. government's operations. Digital services have become increasingly important for various agencies to perform their core missions. The internet provides the means for veterans to claim their benefits and for citizens to register to vote. It is increasingly the medium used for government to communicate with citizens, particularly in emergencies. And it provides the means for citizens to find and sign up for healthcare plans. Healthcare.gov, the online healthcare marketplace for President Barack Obama's signature initiative, is a prime example of the importance the internet and digital services have taken in government operations, as well as a cautionary example of what can happen when those digital services fail.

This dependence is present in the national security organs of government as well. Though intelligence agencies and the Department of Defense generally hold their networks to a higher security standard, relying on private networks disconnected from the internet for the most important missions, no modern institution can be entirely self-sustaining and firewalled from global communications. Agencies, even secretive ones, need to communicate and contract with outside entities, including private sector suppliers, to ensure the availability of basic necessities like power and water. The Department of Defense relies overwhelmingly on commercial networks for its logistics functions, without which the military may face serious challenges in a contingency.

Threats to Core Internet Infrastructure and Services

A variety of attacks could pose systemic risk to the normal functioning of the internet. This section will describe some of the most prominent and recently observed, but the variety of attacks are as diverse and dynamic as the internet itself.

Border Gateway Protocol Hijacking

The Border Gateway Protocol (BGP) is vital for the global routing of internet traffic. BGP helps a packet find the quickest route from its origin to its destination. When a user's request reaches a router, BGP provides a formula to identify the next router to which to pass the user's request, and on and on until the request reaches its destination. Famously, the protocol was devised on the back of a napkin to provide a quick-fix in 1989; against all odds it is now the internet standard, required for use by major internet service providers.[12] BGP runs on trust – each router running BGP must trust the announcements from other routers in the chain about where traffic should be sent. Today, this trust is frequently exploited.[13]

The most notorious case of BGP hijacking was unintentional. In 2008, the Pakistani government attempted to block YouTube in the country after taking offense to a video posted on the site. The internet service provider in Pakistan misconfigured its BGP instructions, issuing a message to other routers that requests for the internet protocol (IP) address corresponding to YouTube.com should be routed through the Pakistan provider. Because the protocol relies on trust, global requests for YouTube immediately started flooding this Pakistani provider – overloading the local provider and rendering YouTube inaccessible for two hours until the error was fixed.[14]

12 Craig Timberg, 'The Long Life of a Quick 'Fix'," The Washington Post, 31 May 2015.

13 For an excellent study on the prevalence of BGP hijacking, see Pierre-Antoine Vervier, et al, 'Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks,' The Network and Distributed System Security Symposium, The Internet Society, 2015.

14 Timberg, 'The Long Life of a Quick 'Fix'.

BGP can also be intentionally hijacked. In 2013, multiple Belarusian internet providers sent a number of fraudulent BGP announcements that resulted in domestic U.S. traffic (like a user in Oklahoma visiting a site hosted in Ohio) taking a slight "detour" through Minsk and Moscow.[15] Most observers at the time believed the incidents occurred too frequently to be accidental, and many feared that it could have enabled the collection of massive amounts of U.S. traffic by hostile intelligence services. This was not the first time that a BGP redirection raised concerns of nation-state tampering. Several years earlier, roughly 15% of U.S. internet traffic – including military and government communications – was improperly routed through Chinese servers.[16] Attacks continue to this day. On April 26, 2017, a Russian-government controlled telecommunications provider routed the traffic from over two dozen major financial sector companies through its networks for five to seven minutes. [17]

As these examples demonstrate, BGP hijacking can be used to create multiple effects. Traffic can be diverted to a "sink-hole," slowing it to a standstill and denying service to portions of the web, or it can be diverted to friendly infrastructure where it can be collected for intelligence purposes. While routing companies can swiftly take steps to block these actions, as was the case for the YouTube incident, even short disruptions can be used to significant effect.

Certificate Authority Compromise

Today, when a user visits a website, the user's browser exchanges digital certificates with that website to ensure that the user and the company hosting the website are both who they claim to be, and to encrypt the communications between user and server. These certificates are generally issued by root certificate authorities, which design and implement the encryption scheme for much of the web. In short, certificate authorities are critical for ensuring the confidentiality and integrity of much of the data on the internet.

15 Kim Zetter, 'Someone's Been Siphoning Data Through a Huge Security Hole in the Internet,' Wired, 5 December 2013.

16 Dugald McConnell, 'Report: Chinese company 'hijacked' U.S. web traffic,' CNN, 18 November 2010.

17 Dan Goodin, 'Russian-controlled telecom hijacks financial services' Internet traffic,' Ars Technica, 27 April 2017.

When a certificate authority is compromised, attackers can issue fraudulent digital certificates. This allows attackers to compromise the secure connection between user and server and access the communications (known as a man-in-the-middle attack).

The most significant known certificate authority compromise was discovered in 2011 when an attacker compromised DigiNotar, a root certificate authority in the Netherlands. The attacker began issuing fraudulent certificates, including for Google, Yahoo!, and Mozilla.[18] This attack reportedly compromised 300,000 Google users in Iran alone, enabling attackers to gain direct access to the victims' accounts.[19]

DigiNotar was a relatively small certificate authority, and the market is dominated by a few large authority providers, including Symantec, GoDaddy, and Comodo.[20] Compromise of any of these authorities would have far more severe consequences for global trust and confidence in the internet. Concerns abound. Symantec recently admitted that several employees issued unauthorized certificates for Google without Google's knowledge.[21] Google's concerns about the certificate authority ecosystem led the company to recently create their own root authority – freeing them from reliance on external certificate authorities altogether.[22] In addition, Google sponsors the Certificate Transparency project, an open standard and open-source framework that helps identify malicious certificates.[23] Google recently announced that its widely-used browser, Chrome, will begin enforcing Certificate Transparency in October 2017.[24] These are notable, important steps taken by a major internet company to incentivize increased security measures in other companies.

---

18 Associated Press, 'Hacking in the Netherlands Took Aim at Internet Giants,' The New York Times, 5 September 2011.

19 'Iranians hit in email hack attack,' BBC News, 6 September 2011.

20 For an updated list of certificate authority usage across the internet, see 'Usage of SSL certificate authorities for websites,' World Wide Web Technology Surveys.

21 Dan Goodin, 'Symantec employees fired for issuing rogue HTTPS certificate for Google,' Ars Technica, 21 September 2015.

22 Ryan Hurst, 'The foundation of a more secure web,' Google Security Blog, 26 January 2017.

23 'Certificate Transparency,' Google Transparency Report.

24 Ryan Sleevi, 'Announcement: Requiring Certificate Transparency in 2017,' Google Groups, 24 October 2016.

Threats to cables

Attacks on the internet need not be launched from computers. Physical threats to the infrastructure that transmits communications are as old as communications itself. In the internet age, physical disruption to the fiber-optic cables carrying internet traffic has at times had profound effects on internet users. Most of these instances occur when the long-haul trans-oceanic undersea cables are inadvertently cut, such as by a ship's anchor or fishing net.[25] Some cable cutting instances have been intentional, however. Fiber-optic cables in the San Francisco area were cut at least eleven times between 2014 and 2015, causing regional internet disruptions.[26] In 2015, an unknown attacker shot a fiber-optic cable in Navajo County, Arizona, leaving residents without access to the internet or to 911 emergency services for nearly a day.[27]

Most recently, Russian activities have raised concerns amongst U.S. officials. Russia has been observed aggressively operating ships and submarines close to major undersea cables, renewing concerns about the vulnerability of this infrastructure in a conflict.[28] According to *The New York Times*, Pentagon officials are concerned that the Russians are searching for undersea cable vulnerabilities at greater depths, where severed cables are far more difficult to repair.[29]

Domain Name System threats

The domain name system (DNS) is often referred to as the internet's phone book; at its core, it is the service that matches human-readable websites (e.g., Google.com) with its computer-readable internet protocol address (e.g., 216.58.217.110). The system itself is far more complicated than a

25 Greg Miller, 'Undersea Internet Cables Are Surprisingly Vulnerable,' Wired, 29 October 2015.

26 Shane Harris, 'Who's Cutting California Internet Cables? The FBI Has No Idea,' The Daily Beast, 4 July 2015.

27 The Associated Press, 'Ruptured cable cripples Internet, 911 calls in Navajo County,' Fox 10, 22 July 2015.

28 David E. Sanger and Eric Schmitt, 'Russian Ships Near Data Cables Are Too Close for U.S. Comfort,' The New York Times, 25 October 2015.

29 Ibid.

book matching names to numbers, however. The authoritative "phone books" at the top of the naming hierarchy are hosted on root name servers. There are 13 root name servers, which collectively return IP addresses or referrals to subordinate name servers for all possible website lookups to any user or internet-connected application across the globe. There are other DNS servers in the hierarchy as well, because the root server knows *where* the proper IP address is located, but it does not itself possess the record. When a user makes a lookup request, an intermediary ("recursive") DNS server will ask the root server to point it to the proper authoritative name server, which will have the specific match between website and IP address or provide a referral to other name servers that provide the answer. Once the website's IP address is saved (cached) by the user's browser or the recursive server, it can return users to the website without using DNS for a certain period of time.

Like many other aspects of the internet, key portions of the domain name system's architecture and administration is managed in a global multi-stakeholder governance model. A private non-profit corporation, the Internet Corporation for Assigned Names and Numbers (ICANN), operates as the Internet Assigned Numbers Authority, which entails allocating IP addresses and administering the root zone file at the top of the domain name hierarchy. Carrying out these functions involves closely collaborating with the national service providers across the globe, foreign governments, and the international community of internet experts. Previously, ICANN performed this service under contract to the U.S. government, which led detractors to claim that the internet's architecture and policy was unduly influenced by the U.S. In October 2016, the Department of Commerce ended the contract, leaving the administration of the domain name service entirely in the hands of a non-governmental community.[30]

Needless to say, the internet would cease to exist without DNS; it is what unifies the loosely interconnected network of networks that makes up the internet. Without it, users would be unable to visit any websites because the user's computer would not know where to find them. DNS is a resilient,

30 'Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends,' International Corporation for Assigned Names and Numbers, 1 October 2016.

distributed system, but attackers have successfully exploited or degraded specific portions of DNS in the past.

Common attacks on DNS typically involve swapping legitimate DNS records for fraudulent records controlled by the attackers. These attacks, called DNS poisoning or spoofing, occur when an attacker is able to manipulate the cache of the browser or recursive name server, so that when a user's browser requests the IP address for a site, the attacker's IP address is returned – sending the user to a malicious site that can compromise the user. This kind of manipulation generally targets recursive name servers – the DNS resource closest to the user that is generally operated by the local internet service provider. This means the effects are relatively localized. Compromise of authoritative server records, however, is far more serious and global in scope. For instance, in 2013, the Syrian Electronic Army (SEA) hacked into the domain registration accounts of Twitter and the *New York Times*, changing the authoritative name server locations to domains operated by SEA.[31] For several hours, and in some cases for a full day, all visitors seeking to visit those sites were rerouted to malicious pages. More recently, in October 2016 hackers compromised a Brazilian bank's domain registration account to seize control of the bank's websites and intercept its customers' ATM, point-of-sale, online banking and investment transactions.[32] Though these were serious breaches, even more serious would be a takeover of the authoritative servers themselves. While compromising an individual customer's registration account allows attackers to manipulate that customer's web traffic, compromising the authoritative server where these registrations take place would compromise all customers. Compromising the authoritative top level domain server for .com, for instance, could allow attackers to manipulate traffic for any .com website.

While the aforementioned attacks stealthily reroute users to fraudulent sites, other types of attacks simply block access to the domain name system, making it impossible for users to access websites. Most recently, the vulnerability of DNS to distributed denial of service attacks has re-emerged as a major issue. This is primarily due to the proliferation of connected consumer devices that are directly accessible from the internet and shipped

31 'DNS Security: Three Ways That Hijacks Can Happen,' Dyn Blog, 28 August 2013.

32 Andy Greenberg, 'How Hackers Hijacked a Bank's Entire Online Operation,' Wired, 4 April 2017.

to consumers with insecure network interfaces. Hackers have developed malicious software to automatically compromise hordes of these devices—including digital video recorders and webcams—over the internet and put this network of compromised devices ('botnets') to malicious use. These botnets have been used to generate tremendous amounts of internet traffic on a scale far larger than DDoS attacks of the past; under well-targeted attacks, this traffic has caused even the largest enterprises to buckle for periods of time. Though there are various DDoS mitigation techniques to filter out the malicious requests, beyond a certain point network defenders have to use a butcher knife, rather than a scalpel, to cut off the traffic—impacting both legitimate and malicious traffic.

When these new Internet-of-Things-powered botnets are turned against DNS and other core internet services, the results have been serious. The most notable instance was in October 2016, when the most prominent botnet, Mirai, and others were used to target Dyn, a major provider of DNS and traffic management services. Dyn provides authoritative DNS services for millions of domain names, including many of the top websites in the United States, such as Twitter, Netflix, Amazon, and Spotify. On October 21, a DDoS attack against Dyn's DNS infrastructure first targeted Dyn's U.S. East Coast data centers, making their customers' sites inaccessible for East Coast users, then later targeted Dyn's global data centers, causing further inaccessibility. Some of the customers, like Amazon, were able to switch to a backup DNS provider, mitigating the impact. Others, such as PayPal, did not have a secondary provider—though PayPal purchased those services by the end of the day.[33] This is another example of the importance of backups and resiliency to prevent cascading failure.

Other recent DDoS attacks against different components of the internet's infrastructure have heightened concerns. Prior to the Dyn attack, the Mirai botnet was used to attack the website of prominent information security journalist Brian Krebs. Krebs used, on a pro-bono basis, the services of major content delivery firm Akamai. This attack strained Akamai's servers (whose network is so large it is responsible for roughly 15-30% of daily internet traffic[34]), enough that the company ended up severing its relation-

33 Tim Greene, 'How the Dyn DDoS attack unfolded,' Network World, 21 October 2016.

34 'Visualizing Global Internet Performance,' Akamai.

ship with Krebs.[35] The attack on Krebs was estimated to have generated 620 Gigabits-per-second (Gbps) of internet traffic – a record at the time. Following this attack, the source code for Mirai was leaked online, allowing the malware to proliferate. A month later, the Dyn attackers reportedly generated 1.2 Terabits-per-second (Tbps), twice as strong as the attack on Krebs.[36] Another noteworthy use of the botnet took place in November against Deutsche Telekom – Germany's largest telecommunications company and internet service provider. This attack, which also used the Mirai botnet and targeted insecure Deutsche Telekom routers, reportedly knocked 900,000 customers offline.[37]

Unfortunately, the rise of IoT devices means this trend may get worse before it gets better. More and more devices are being manufactured, sold, and then connected to the internet—various studies estimate the number of internet-connected devices in 2016 from 6.4 billion to 17.9 billion, and those same studies project numbers will reach between 20.8 billion and 30.7 billion by 2020.[38] This profusion is not inherently bad for society. But these devices tend to be shipped with a poor level of security, and neither the producers nor the consumers have adequate incentives today to make them more secure. While security firms will continue to generate new DDoS mitigations, defending against these attacks still comes down to whether the defender can absorb more than the attacker can launch. With botnets such as Mirai able to take advantage of more and more devices to generate ever greater volumes of traffic, risk to core internet infrastructure may grow in the next several years.

35 Brian Krebs, 'Akamai on the Record KrebsOnSecurity Attack,' Krebs on Security, 22 November 2016.

36 Nicky Woolf, 'DDoS attack that disrupted internet was largest of its kind in history, experts say,' The Guardian, 26 October 2016.

37 Eric Auchard, 'Deutsche Telekom attack part of global campaign on routers,' Reuters, 29 November 2016.

38 For a discussion of various high and low estimates of connected devices, see Amy Nordrum, 'Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated,' IEEE Spectrum, 18 August 2016.

Nation State Intentions and Capabilities

Much of the scholarship and debate on nation state conflict in the cyber domain focuses on high-end malware-based attacks on critical infrastructure (power, water, emergency services, etc.) and military platforms.[39] While these techniques are no doubt concerning, nation states have amply demonstrated interest and willingness to use attacks on core internet infrastructure to achieve their end goals as well. Internet infrastructure attacks may be attractive to states for a number of reasons.

First, many of these attacks do not rely on access to execute. Gaining access to the target system in cyber operations is often the most challenging step. It may involve months or years of reconnaissance, and it often relies on the victim user to make a bad decision (e.g., clicking a malicious link). But once an attacker has persistent administrative access to a target, the desired effect is frequently trivial to achieve. However, a denial of service attack on the domain name system requires no direct access to the victim at all. DNS is a global service and the IP addresses for root and authoritative name servers are readily apparent. For a denial of service attack that takes systems off-line, an attacker simply needs to aim its botnet at the target and launch the attack – no compromise or direct system access required.

Many of these attacks are also easily reversible, which is key to their coercive power. This is one reason why the Mirai botnet is being used to extort money from victims[40] – it can be turned off with the push of a button. If the victim state knows that an attack can be reversed if the attacker's demands are obeyed, it may be more likely to do the attacker's bidding. Using DDoS to compel a defender to do the attacker's bidding is a well-known tactic for 'hacktivists,' including many suspected proxies for nation states. Many politically-motivated DDoS attacks come with a statement from a shadowy

39 Evidence abounds that the U.S. government, historically, focused on high-end cyber attacks, potentially at the expense of a focus on less damaging but more likely threats. Several examples: Elizabeth Gurdus, 'We're headed for a 'cyber Pearl Harbor,' says Adm James Stavridis,' CNBC, 15 December 2016; Sean Lawson, 'Does 2016 Mark the End of Cyber Pearl Harbor Hysteria?,' Forbes, 7 December 2016; and Elisabeth Bumiller and Thom Shanker, 'Panetta Warns of Dire Threat of Cyberattack on U.S.,' The New York Times, 11 November 2012.

40 Roi Perez, 'Digital Shadows says DDoS extortion on the rise thanks to Mirai botnet,' SC Magazine UK, 14 December 2016.

organization that claims responsibility and makes demands of the victim as a precondition to ending the attack. For example, the Ukrainian hacker group Cyber Berkut launched a denial of service attack on NATO websites in 2014 to protest a NATO delegation's visit to Ukraine and call for the delegation's expulsion.[41]

Finally, because these attacks are reversible, seldom cause lasting damage, and are less intrusive since they do not require access, they may be viewed as less escalatory than attacks that actually destroy physical hardware, such as the destructive attack against energy firm Saudi Aramco in 2012, which destroyed tens of thousands of computers. This makes them an attractive option for nations seeking to make a point but hesitant to get in a hot conflict with a stronger opponent.

Suspected Attacks

Nation states have clearly taken note and incorporated disruptive attacks in their cyber operations toolkit. Attacks disrupting major communications networks in a victim country are consistent with the military doctrine of a number of major powers. Over the past decade, a variety of countries have shown a willingness to tinker with core internet services and infrastructure. For some, these operations occur frequently enough that they appear to be a key component of these nations' cyber operations strategy.

Iranian hackers have used DDoS as a tool to disrupt adversary networks for years, though they most often attack specific targets of their ire versus internet infrastructure. Iran's most notable cyber campaign, Operation Ababil, targeted major U.S. financial institutions on a weekly basis from 2011-2013.[42] These attacks disrupted the online banking sites for JP Morgan Chase, Bank of America, and others, as well as institutions like the New York Stock Exchange. Since then, Iran is suspected of carrying out similar attacks against other adversaries, including Israel and Saudi Arabia.[43]

41 Adrian Croft and Peter Apps, 'NATO websites hit in cyber attack linked to Crimea tension,' Reuters, 16 March 2014.

42 Nicole Perlroth and Quentin Hardy, 'Bank Hacking Was the Work of Iranians, Officials Say,' The New York Times, 8 January 2013.

43 David Shamah, 'Official: Iran, Hamas conduct cyber-attacks against Israel,' 13 August 2015.

The People's Republic of China has also turned to disruptive attacks on the internet. In 2015, the Chinese government, always concerned about their citizens accessing objectionable content, conducted a DDoS attack on GitHub, the popular project hosting company. The attack targeted sites GitHub was hosting that helped people evade Chinese censorship, including a mirror of the *New York Times*' China edition, and another site that helped users evade China's Great Firewall.[44] Noteworthy here is that the attack tool, called the Great Cannon, was co-located with the Great Firewall, China's national traffic monitoring system, and it repurposed legitimate inbound traffic to attack the offending sites.[45] This was a highly significant event in the evolution of the threat: a sovereign state turned the entire infrastructure of its domestic internet into an offensive weapon. While this tool has not been observed in action since that event, and it did not target national infrastructure, its use set an example that others may follow in the future.

Other attacks and attackers have utilized these same techniques to target core infrastructure and cause widespread connectivity disruption.

More than any other nation, Russia appears to have taken to attacks on core internet infrastructure with gusto. Though publicly attributing responsibility for specific attacks remains a challenge, Russia's antagonists always suffer from denial of service attacks on their top government and civil society institutions. Whether the hackers are directly tasked by the Russian government or not is almost beside the point: if the Russian government makes a major foreign policy decision or condemns another state's actions, denial of service attacks follow. The most significant attacks have come during major disputes and conflicts over the past ten years. Perhaps most notable was the massive DDoS attacks against Estonia in 2007. These attacks, launched in protest of an Estonian decision to move a memorial to fallen Soviet soldiers, targeted Estonia's domain name servers, major banks, government, and news services.[46] In that case, the attacks were so overwhelming that the Estonian

44 Dan Goodin, 'Massive denial-of-service attack on GitHub tied to Chinese government,' Ars Technica, 31 March 2015.

45 Marczak and Weaver et al, 'China's Great Cannon'.

46 An excellent overview of the Estonian cyber attacks may be found in the first section of Eneken Tikk, Kadri Kaska, and Liis Vihul, 'International Cyber Incidents: Legal Considerations,' NATO Cooperative Cyber Defence Centre of Excellence, 2010.

government decided to sever Estonia's connection to the global internet–meaning news could get neither in nor out.[47]

Similar attacks surfaced during Russia's 2008 conflict in Georgia. Their use in this conflict was notable because the attacks seemed synchronized with full spectrum operations conducted by the Russian military. As Russian forces invaded the country, DDoS attacks suppressed communications networks and media organizations at a time when they were most needed by the Georgian government and citizens.[48] The government was unable to communicate with its citizens effectively, and the news blackout hurt Georgia's ability to galvanize a response from the international community. As hostilities with the West rose in recent years, Russian internet attacks have proceeded apace. The Ukraine incursion, in particular, has led to significant cyber operations and activities to disrupt the internet. During the seizure of Crimea, suspected Russian operatives seized control of Crimea's service providers and tampered with the cables, causing selective outages across the country.[49] Elsewhere, hackers not only targeted Ukrainian institutions, including its electoral commission, but, as previously mentioned, also conducted attacks against NATO's websites in connection with the incursion.[50, 51]

No example captures the potential of these attacks better than the attack against Turkey's internet backbone in December 2015. Hackers launched attacks against Turkey's five name servers administering its top level domain country code (.tr), and also targeted the secondary name servers administered by the European regional internet registry.[52] As the defenders responded, the attacker changed the traffic pattern to evade the mitigations.[53] This attack blocked access for at least a day to *all* sites using Turkey's top level domain, which included most banks and media

47 Joshua Davis, 'Hackers Take Down the Most Wired Country in Europe,' Wired, 21 August 2007.

48 A good case study on the use of cyber operations in the Georgia conflict may be found at David Hollis, 'Cyberwar Case Study: Georgia 2008,' Small Wars Journal, 6 January 2011.

49 Chelsea J. Carter, Ingrid Formanek, and Diana Magnay, 'Obama warns Russia against Ukraine intervention, says 'there will be costs'," CNN, 28 Febuary 2014.

50 Croft and Apps, 'NATO websites hit in cyber attack linked to Crimea tension.'

51 Mark Clayton, 'Ukraine election narrowly avoided 'wanton destruction' from hackers,' Christian Science Monitor, 17 June 2014.

52 Efe Kerem Sozeri, 'Turkish Internet hit with massive DDoS attack.'

53 Romeo Zwart, 'RIPE NCC Authoritative and Secondary DNS services on Monday 14 December,' RIPE Network Coordination Centre, 15 December 2015.

and all government and military networks within the country. The attacks continued for two more weeks, though it is unclear if the same attacker was responsible for all the attacks. While attribution of the initial attack remains publicly unknown, many believe that Russian-backed hackers conducted the attack in response to Turkey's shoot-down of a Russian fighter aircraft a few weeks earlier.[54] This attack was quickly overshadowed by the dramatic attack on Ukraine's electric grid later that month, but the attack on Turkey's telecommunications backbone both lasted longer and had arguably more significant effects.

Russian operations are not limited to DDoS attacks on internet infrastructure, of course. Russian intelligence services would be the most likely culprit behind the aforementioned BGP hijacking that redirected domestic U.S. traffic to Minsk and Moscow, for example. While this operation would have been for intelligence collection, the technique could also be used to cause disruptions in U.S. traffic.

National Internets as Walled Gardens

China, Russia, Iran, and North Korea are also shielding their own national internets from these same attacks. Attacks with regional or global effects become all the more attractive if aggressors are shielded from its collateral effects. Several nations are investing in telecommunications architectures that would wall their domestic internet off from the rest of the world. While this may lead to internal infrastructure that is less advanced, more brittle, and susceptible to degraded service, it may be more difficult to attack from abroad.

China's Great Firewall is the most prominent example of this. The Great Firewall refers to an extensive web of network surveillance and control capabilities (much of it, for now, supplied by U.S. firms) allowing the Chinese government to surveil its citizens and block content and websites deemed objectionable.[55] But other nations are taking similar steps. Following the Snowden revelations, Brazil began laying its own internet cables to

54 Efe Kerem Sozeri, 'Turkish Internet hit with massive DDoS attack.'

55 Geremie R. Barme and Sang Ye, 'The Great Firewall of China,' Wired, 1 June 1997.

avoid surveillance by U.S. intelligence.[56] And Iran, too, has been building what it calls a "Halal internet," separate from the rest of the globe, with its own approved content.[57]

Russia has recently been making waves along these lines. Their strategy has several components, including building domestic alternatives to popular hardware and software products, kicking Western businesses out of the country, and forcing companies to store user data inside Russia. Russia has turned to Chinese companies for help building a Great Firewall analogue, and the two nations signed a pact in 2014 to jointly develop related technologies. Former House Intelligence Committee Chairman Mike Rogers commented at the time that Russia and China were, "creating this alternative out there…to what we would know as the Internet."[58]

A variety of factors drive these activities. First, nations like China and Russia want greater government control over the information their citizens can access online and the ability to censor content. Second, nations are concerned that Western technologies are clandestinely manipulated by intelligence services, particularly from the United States, to spy on their regimes.[59] For some of these states, the global internet is not a force for good—it is a force that undermines the social cohesion and harmony in their country by introducing harmful influences.

These nations may have far less compunction about conducting attacks that would lead to global disruption, particularly if they perceive themselves as immune to the disruption due to walled-off domestic internets. If attacks on the internet routing system, global DNS infrastructure or certificate authorities come with no collateral damage to their social, governmental, or military networks, nations may view these attacks more attractively, doubly so if they believe their own tightly-controlled networks are less susceptible to attacks from abroad.

56 Nancy Scola, 'Brazil begins laying its own Internet cables to avoid U.S. surveillance,' The Washington Post, 3 November 2014.

57 Daisy Carrington, 'Iran tightens grip on cyberspace with 'halal internet'," CNN, 3 June 2013.

58 Cory Bennett, 'China, Russia seeking their own Internet, warns former Intel chairman.'

59 Elizabeth Dwoskin, 'New Report: Snowden Revelations Hurt U.S. Companies,' The Wall Street Journal, 30 July 2014.

Use in a Conflict

As a nation dedicated to an open internet policy with a society deeply dependent on connectivity, the United States is particularly vulnerable to attacks on core internet infrastructure. The U.S. cannot afford to think of these attacks as a method only used by mischief makers or criminals. Serious adversaries may turn to these attacks to deter the U.S., control escalation in a crisis, or even help defeat the U.S. military in a full blown conflict.

An attack on core internet infrastructure may not be itself decisive in a conflict with the United States, but it would not need to be. Speed and seizing the information high ground has proven decisive in conflicts in the twenty-first century, and attacks on core internet infrastructure would sow confusion and hurt the U.S. military's ability to react and respond quickly. Russia has proven adept at suppressing the communications links of adversaries at the outset of a conflict to create and exploit uncertainty before victims can react. In the Crimean invasion in March 2014, for example, Russia used physical access to internet and telecommunications infrastructure to sever cable connections between Crimea and the rest of Ukraine and the world, hurting the Ukraine government's ability to respond quickly and allowing Russia to dictate the narrative.[60] While Ukraine and the international community attempted to discern what was happening, Russian forces had already moved into the country and established the facts on the ground. Russia used cyber operations for similar purposes in Estonia and Georgia. In modern warfare, speed and surprise are critical and attacks on U.S. internet infrastructure could put the American government on the back foot at the wrong moment.

Attackers would have several targets to exploit at the outset of a conflict. First, adversaries may be able to directly degrade or disrupt U.S. government networks, including those of the military. The Department of Defense operates its own vast, private network for sensitive but unclassified communications. This network, called the Non-secure Internet Protocol Router Network (NIPRNet), is logically separated from the global internet

60 Bettina Renz and Hanna Smith, 'Russia and Hybrid Warfare – Going Beyond the Label,' Aleksanteri Papers vol. 1/2016, Kikimora Publications, Aleksanteri Institute, University of Helsinki, Finland. Pp. 44-45.

but connected, allowing properly-authenticated DoD users to access the internet. A different network for classified networking, called the Secret Internet Protocol Router Network (SIPRNet) is further separated and does not permit broader internet access.[61] While classified networks are used for the most mission-critical communications and functions (for instance, actual command and control of forces), NIPRNet is responsible for many business processes at the Department and much of the day-to-day communication.[62]

To facilitate routing within NIPRNet, DoD operates its own domain name service with its own root server for the .mil top level domain.[63] That DoD's DNS infrastructure is inside the boundary of NIPRNet means that it would be difficult for an attacker to brute force DoD's DNS directly. NIPRNet users must have a valid common-access card to access NIPRNet resources; remotely flooding DoD's name servers would be difficult without this access.

However, indirect attacks may have a similar impact. For instance, according to the Defense Science Board, much of the Defense Department's connectivity is commercially provided.[64] Commercial internet service providers carry military traffic, meaning targeted disruptions of those carriers may indirectly disrupt the military's routing.

An attacker would not need to disrupt military communications directly to hurt U.S. defense efforts, however. Much as the Estonians chose to cut themselves off from the global internet in 2007, an assault on the U.S. military's internet connectivity could lead military decision makers to pull up the drawbridge and sever the Defense Department from broader internet access. This would protect core internal communications and computing, but the military's global communications interdependencies means that

61 'Using the SIPRNet,' Online Guide to Security Responsibilities, Defense Personnel Security Research Center, Department of Defense.

62 While there is no public authoritative data regarding which functions (and corresponding systems) are conducted on NIPRNet versus SIPRNet, cursory web searches show that a diverse array of systems are accessible via NIPRNet, including systems tracking global personnel accountability, DoD personnel travel, mobilization of personnel and equipment, payroll*, and weather data.*

63 'Internet Domain Name and Internet Protocol Address Space Use and Approval,' Department of Defense Instruction Number 8410.01, Department of Defense, issued 4 December 2015.

64 'Protecting the Homeland,' Report of the Defense Science Board, 2000 Summer Study, Executive Summary, Volume 1. *Pp. 11.*

this move would not come without cost. Whether or not an attack could affect the military's own network, the U.S. military relies on external connectivity and communications to function. This includes communications with allied governments, interagency partners, and the private sector. Severing the military from the internet would have broad impacts to a number of the military's key and enabling missions.

As a prime example, the military would be hard pressed to move its materiel and personnel around the world without internet connectivity. The military's mobility and logistics capabilities are heavily reliant on commercial partners and networks. In 2013, U.S. Transportation Command (USTRANSCOM), the operational command within the U.S. military responsible for global mobility, assessed that 70% of its supplies and passengers were moved by commercial partners, and that 90% of its transactions for logistics and deployments took place over commercial and unclassified networks without the protections of the NIPRNet.[65] A 2014 investigation by the Senate Armed Services Committee focusing on intrusions in USTRANSCOM contractor networks found that "the private sector plays a crucial role in force mobilization, deployment, and sustainment operations and the overwhelming majority of Department of Defense deployment and distribution transactions occur over unclassified networks, many of which are owned by private companies".[66] The Committee further found that USTRANSCOM had difficulty even identifying which commercial relationships would be critical in a contingency. Part of the difficulty in identifying dependencies on the private sector is that those dependencies are not apparent in peace time, and only become critical in a contingency. For instance, the Department's civil-reserve air fleet consists of private sector airliners that augment DoD's airlift capacity with their commercial fleet during emergencies such as war or natural disaster. American Airlines may never be needed by the military until a true conflict broke out, at which point their fleet would provide critical surge support to fly personnel and materiel to theater. An inability to communicate with those operationally-critical contractors in the run-up to a contingency would pose a substantial risk to military operations.

65 Donna Miles, 'Transcom, Partners Secure Networks Against Cyberattacks,' American Forces Press Service, Department of Defense, 7 March 2013.

66 'Inquiry Into Cyber Intrusions Affecting U.S. Transportation Command Contractors,' Report of the Senate Armed Services Committee, 2014. Pp. viii.

Beyond effects on military communications, much of U.S. critical infrastructure owners and operators' reliance on internet connectivity could prove to be a strategic vulnerability that an adversary can exploit. Attacks targeting domestic commercial internet connections could have far reaching and little-understood consequences. Though Americans can likely make do without Netflix and Twitter for some time, domestic internet outages would also impact emergency services and communications in a crisis. This could amplify the effect of attacks in other domains and complicate the response. The chaos that would ensue could hurt U.S. cohesion and resolve at a decisive time and allow an adversary to force the U.S. to back down.

Finally, attacks would not need to target U.S. connectivity at all to threaten U.S. interests. Internet outages in key theaters where the U.S. military is operating could degrade U.S. capabilities. And attacks on allied networks at the outset of a conflict could hurt the United States' ability to live up to its defense commitments in places like the Middle East, Eastern Europe, and East Asia, where the U.S. and allies would be vastly outnumbered at the outset of a conflict. In a conflict over Taiwan, for example, U.S. strategists have long been concerned that disruptive attacks on communications networks could provide the window needed by China to seize the initiative and force Taiwan to surrender before the U.S. is able to react.[67]

67 One example: 'China's Military Modernization and Cross-Strait Balance,' Transcript from the Hearing before the U.S.-China Economic and Security Review Commission. 15 September 2005.

Safeguarding the U.S. from Threats to Core Internet Infrastructure: Recommendations

The deep penetration of network connectivity in American society, government, and critical infrastructure make this a difficult threat to wrestle with for the United States government, and following China and Russia's lead to build a wall around domestic connectivity cannot be the solution. The global internet is a significant driver of American economic growth and efficiency and has major social and cultural benefits. And not least of all, a free and open internet is consistent with American values. This level of connectivity and engagement is a net positive for American society, and reducing that connectivity cannot be the solution except, perhaps, in niche areas of the economy.

Solutions raised in the context of Mirai botnet attacks have focused on preventing or building defenses against that specific attack vector. In particular, many have focused on improving IoT device security so these connected devices cannot be compromised *en masse*. Popular solutions include ensuring devices no longer ship with default passwords and are able to be patched over time.[68,69] Some have called on international standards bodies such as the Institute of Electrical and Electronics Engineers to lead the effort to define the most important security standards. Others have proposed building smarter networks to distinguish normal IoT network activity from abnormal activity, and some have called for the creation of separate non-TCP/IP based IoT networking protocols to ensure IoT devices cannot target normal internet-connected resources.[70,71] Some have called for increased regulation of device manufacturers or imposing

68 Alan Grau, 'IoT Security Standards – Paving the Way For Customer Confidence,' IEEE Standards University, 29 February 2016.

69 'Internet of Things: Privacy and Security in a Connected World,' FTC Staff Report, Federal Trade Commission, January 2015.

70 Liang Zhou and Han-Chieh Chao, 'Multimedia Traffic Security Architecture for the Internet of Things,' IEEE Network, May/June 2011.

71 Ari Keranen and Carsten Bormann, 'Internet of Things: Standards and Guidance from the IETF,' IETF Journal, Volume 11, Issue 3, April 2016.

additional legal liability.[72,73] Finally, many are calling on traffic carriers and networking companies to improve their own defenses against massive botnet attacks and build more capacity.[74]

Others have proposed solutions to better secure key protocols, including BGP and DNS, that power the internet. International standards organizations have proposed updates to BGP and DNS that would provide, among other things, better security and authentication so that malicious actors cannot manipulate traffic and conduct attacks such as BGP hijacking and DNS spoofing. Both of these updates (BGPsec and DNSSEC) face a long road to widespread adoption, and introduce new complexities and vulnerabilities themselves. For the vast majority of the time, the original protocols work as intended, and the new ones will cause growing pains. Shifting to new protocols is a generational endeavor.

The aforementioned proposals are important, but they all seek to address specific technical issues surrounding security risks, rather than the deeper issue of interdependencies between the internet and critical infrastructure. A broader set of solutions are needed to ensure that the United States is prepared to confront significant internet outages in a conflict.

Raise Awareness

The first step for addressing any problem is recognizing it and defining its scope. The reliance of critical infrastructure and government functions on network connectivity is still poorly understood and accounted for in a variety of crucial areas such as continuity planning, mission assurance, and regulatory affairs. The U.S. needs better methods to survey the state of interconnectivity in the U.S., identify particular areas of vulnerability to core internet infrastructure, and identify critical infrastructure's reliance on it.

72 Amy Nordrum, 'Wanted: Smart Public Policy for Internet of Things Security,' IEEE Spectrum, 10 November 2016.

73 Iain Thomson, 'You know IoT security is bad when libertarians call for strict regulation,' The Register, 15 February 2017.

74 Scott Crawford et al, 'When things attack: Mirai and the Dyn DDoS attack reveal a disturbing future,' 451 Research, 25 October 2016.

One potential solution, proposed by Dan Geer, In-Q-Tel's Chief Information Security Officer, is interconnectivity "stress testing".[75] The recent financial recession led to an increase in government-mandated stress tests for major financial institutions. These tests were designed to identify and mitigate risks arising from the interdependencies in the financial system between large institutions. They tested the financial health of major institutions against major market disruption scenarios to ensure these institutions had enough capital on hand to withstand another crash. Geer proposes a different kind of test: stress testing organizations against major internet outage scenarios (e.g., "the wholesale data loss of a top-three cloud provider," or "a sustained 50 percent drop in available bandwidth") to highlight where mission failure may occur for organizations. Many firms regularly use tools to test the resiliency of their networks against various disruptions as part of their business continuity program, but these tests are generally not required or validated by regulators. Regulators in major critical infrastructure sectors could consider sponsoring these tests. This would have the benefit of helping critical infrastructure owners and operators identify where they must build resiliency, illuminate the scope of the problem for the U.S. government, and could help identify core internet infrastructure and services that are "too interconnected to fail."[76]

With or without such a test, the breathtaking scope of connected devices that tools like Shodan illuminate should give citizens, corporations, and federal agencies pause. The new administration should take steps to build knowledge about the scope of connected critical infrastructure, issue best practices, and develop strategies to roll back connectivity where its use poses unacceptable risks to public safety. The administration's recent executive order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" directs a study group to look at the issue of internet infrastructure resiliency, and is a welcome step. The language establishing the group, however, is narrowly focused on building resiliency against botnets, and does not, on its face, seem to direct efforts to identify interdependencies between the internet and other key sectors. Ideally this group can broaden its focus to make a deeper impact.[77]

---

75 Dan Geer, 'For Good Measure: Stress Analysis,' ;login:, Volume 39, Number 6, USENIX, December 2014.

76 Ibid.

77 'Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,' The Federal Register, 11 May 2017.

Spur the Development and Adoption of Technical Solutions

Many of the attacks mentioned in this paper rely on deficiencies in key network protocols as well as server misconfiguration and other weaknesses to succeed. Although the internet is governed by many stakeholders, not just the United States, the U.S. government can and should do more to strengthen the technical architecture of the internet. The U.S. should play a more active role working with international standards organizations, and it should also actively develop – and share – its own solutions to many of these issues.

The United Kingdom National Cyber Security Centre (NCSC) Active Cyber Defence initiative sets an excellent example here. The U.K. government, through this initiative, is working in partnership with the U.K.'s top service providers to fix problems with software and underlying infrastructure protocols, including BGP, DNS, and Signaling System 7, that are the source of many attacks.[78] In doing so, U.K. government networks will be the first adopter of any solutions that are developed. In the words of Dr. Ian Levy, NCSC Technical Director, "We'll be eating our own dog food to prove the efficacy (or otherwise) of the measures we're asking for, and to prove they scale sensibly before asking anyone else to implement anything."[79] This is an approach the U.S. should take as well. If the U.S. government leads work in this area, others will follow. But if the U.S. is not an active participant, many others will ask why they themselves should get involved.

The Internet as Critical Infrastructure

Particularly as the U.S. administration gains a better sense of risks rising from interconnectivity, the U.S. government should consider the benefits and drawbacks of designating core internet infrastructure as a critical infrastructure sector itself, or clarifying its place within the broader existing communications or information technologies critical infrastructure

78 Ian Levy, 'Active Cyber Defence – tackling cyber attacks on the UK,' National Cyber Security Centre Blog, 1 November 2016.

79 Ibid.

sectors. The IT critical infrastructure sector is so broad as to be meaningless from a risk management and regulatory standpoint, and the communications sector includes major internet service providers, but does not clearly include other key components of the internet ecosystem such as DNS providers. This would doubtlessly be a controversial step – no commercial entity relishes additional government scrutiny – but it could come with benefits.

Whether all the components of core internet infrastructure fall within the legal definition of "critical infrastructure," the administration should consider enhanced engagement and support with internet infrastructure providers to build greater resiliency against attacks on the internet. In particular, the Secretary of Homeland Security should consider including the internet infrastructure community in its "section 9" list. This list, tasked by section 9 of the 2013 executive order 13636 on "Improving Critical Infrastructure Cybersecurity", was developed by DHS and features the critical infrastructure owners and operators whose disruption would be most catastrophic to the country.[80] Companies on this list receive benefits from the federal government above and beyond the norm, including a greater provisioning of security clearances for their personnel to foster greater classified information sharing. Oddly, this executive order exempted all commercial information technology providers from inclusion on the list, an omission which should be fixed. If there are added security benefits from increased collaboration among core internet infrastructure providers and the government, this option should be pursued.

The government should also remain engaged in multi-stakeholder internet governance forums. The transition of Internet Assigned Numbers Authority functions away from U.S. government administration is a positive and remarkable evolution in internet governance, but it should not come with a corresponding decrease in engagement. Staying current and engaged in deliberations involving key services like BGP and DNS will ensure that U.S. interests are accounted for, and will ensure that the U.S. is prepared when any major architectural shifts occur.

80 'Executive Order 13636: Improving Critical Infrastructure Cybersecurity,' The Federal Register, 19 February 2013.

Build Resiliency

The U.S. government should take immediate steps to build resiliency and protect itself against attacks on core internet infrastructure. This threat should be placed in a nation state context and not solely viewed as a tool for non-state groups.

First and foremost, the U.S. government should identify the most critical services on which the military and other key government functions rely and take steps to build redundancy in them. Functions relying on a single source or service provider are often those that are hit hardest when various components and services fail. For example, during the AWS outage in February 2017, companies that did not globally disperse their data storage were hit the hardest.[81] Nowhere is the need for this redundancy more acute than in DNS. The U.S. government should take immediate steps to build redundant internet connections and name service providers for its own networks. Using multiple authoritative name servers from a single provider is not sufficient – organizations should purchase DNS service from multiple providers, too. If one provider fails, as happened during the October 2016 Dyn DDoS attack, web pages will still resolve via an alternative provider's name service. During that attack, sites that used multiple providers were relatively unaffected, while many others were knocked completely offline. Few government networks, if any, currently adhere to this. Adopting these practices will give government a better high ground from which to advocate DNS redundancy adoption amongst critical infrastructure owners and operators.

Given its unique mission in defending the country, the Department of Defense should take additional, extraordinary steps to improve its internet resiliency. In the unthinkable event of its own root name server being destroyed or disrupted, the military will need to find other ways to communicate with its private sector suppliers, other government agencies, and foreign partners. DoD should consider investing in an alternative, private routing structure using an entirely separate infrastructure and provider, known only to itself and these key partners, and activated only during a significant contingency.

81 Wingfield, 'Miscue Calls Attention to Amazon's Dominance in Cloud Computing'.

The U.S. government should also take steps to prepare to lose connectivity and build "muscle memory" to execute its missions in blackout conditions. The recent momentum to bring more government services online is positive, but agencies should not abandon critical paper-based functions just yet, particularly for missions requiring high availability. Civilian departments and agencies should look to the Department of Defense's approach to mission assurance as a model for assuring their own missions. DoD's approach includes identifying the critical functions and assets on which key missions rely; taking steps to protect those assets; and making contingency plans if those assets should fail (i.e., preparing for the worst). The U.S. Navy, for example, recently reinstated celestial navigation in its curriculum after removing it from the curriculum in the 1990s, in the event that an attack made global position systems unavailable.[82] Though the stakes for a mission failure are not as high, perhaps, for civilian agencies as they are for the Department of Defense, all agencies should take steps to protect their ability to carry out their mission in the event of a significant internet outage.

DoD, too, should review its own approach to account for risks from attacks on core internet infrastructure. The 2015 Department of Defense *Cyber Strategy* tasks the Department to expressly integrate cyber risks into its mission assurance program.[83] This should be updated to take into account risks to internet infrastructure in addition to risks to mission critical assets like power and water systems. Military planners and war games should continue integrating and accounting for cyber risks in defense planning efforts.

Norms

Finally, the U.S. and likeminded nations should consider the benefits and drawbacks of advancing an international norm against attacks targeting the internet backbone of another nation in peacetime. A United Nations body has already developed a set of agreed-upon norms of responsible behavior in cyberspace.[84] One of these was a norm against attacks on critical infrastructure in peacetime, but internet-scale attacks on Estonia and

82 Tim Prudente, 'Naval Academy reinstates celestial navigation,' Military Times, 1 November 2015.

83 'The Department of Defense Cyber Strategy,' Department of Defense, April 2015.

84 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,' United Nations General Assembly, 22 July 2015.

Turkey—both of which had nation state fingerprints on them—suggest that this norm may not extend to core internet infrastructure. Fostering an emergent norm against the use of these attacks in peacetime, which could affect millions of innocent civilians, would make them less appetizing to nations valuing their legitimacy on the international stage.

Conclusion

The arguments presented here are not intended to overstate the threat posed from these attacks. In many ways, nations are already in a state of conflict in cyberspace with information confrontation, sabotage, and espionage operations conducted daily. Attacks on core internet infrastructure are not as present a danger as these. But internet attacks would be undeniably attractive to an aggressor in an escalating conflict due to the ease and reversibility of conducting them, and due to the broad disruptions they can cause across key sectors. And among U.S. strategists, these attacks have been overlooked as tools in the toolkit of foreign militaries. High-end destructive attacks that can disable air defense systems and knock planes out of the sky would be highly coveted by any military, but their use is unlikely—they would be extremely hard to pull off, and likely of limited reuse following execution. Attacks on core internet infrastructure provide a bridging option between the grey-zone and hybrid warfare tactics of information confrontation and the high-end offensive cyber operations in a full spectrum war.

Compared to other nations who have been busy building the capability to "opt-out" of the global internet, the U.S. is particularly vulnerable to these attacks. More and more critical functions of our society and economy—banking, emergency services, power, government operations—are choosing to "opt-in" to the global internet, either for remote administration or to provide services. The interdependencies have grown far too complex to understand, and the corresponding risks we run are difficult to estimate. With greater numbers of devices being brought online, and our reliance (and over-reliance) on connectivity to power daily life in America, this problem will only grow more intractable without focused intervention. The

United States should develop strategies to get ahead of this trend by first taking steps to understand the scope of the problem, and then moving to build resiliency around those core internet services that are "too connected to fail." Doing so will ensure the internet remains a positive force in the world.

Notes

Associated Press, 'Hacking in the Netherlands Took Aim at Internet Giants,' The New York Times, 5 September 2011, http://www.nytimes.com/2011/09/06/technology/hacking-in-the-netherlands-broadens-in-scope.html.

Associated Press, 'Ruptured cable cripples Internet, 911 calls in Navajo County,' Fox 10, 22 July 2015, http://www.fox10tv.com/story/29605626/ruptured-cable-cripples-internet-911-calls-in-navajo-county.

Auchard, Eric, 'Deutsche Telekom attack part of global campaign on routers,' Reuters, 29 November 2016, http://www.reuters.com/article/us-deutsche-telekom-outages-idUSKBN13O0X4.

Barme, Geremie R. and Sang Ye, 'The Great Firewall of China,' Wired, 1 June 1997, https://www.wired.com/1997/06/china-3/.

Bennett, Cory, 'China, Russia seeking their own Internet, warns former Intel chairman,' The Hill, 12 May 2015, http://thehill.com/policy/cybersecurity/241759-china-russia-cyber-pact-threatens-internet-says-former-house-intel-chair.

Bumiller, Elisabeth and Thom Shanker, 'Panetta Warns of Dire Threat of Cyberattack on U.S.,' The New York Times, 11 November 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

Carrington, Daisy, 'Iran tightens grip on cyberspace with 'halal internet',' CNN, 3 June 2013, http://www.cnn.com/2013/06/03/world/meast/iran-internet-restrictions-halal-internet/.

Carter, Chelsea J., Ingrid Formanek, and Diana Magnay, 'Obama warns Russia against Ukraine intervention, says 'there will be costs',' CNN, 28 Febuary 2014, http://www.cnn.com/2014/02/28/world/europe/ukraine-politics/.

'Certificate Transparency,' Google Transparency Report, https://www.google.com/transparencyreport/https/ct/.

'China's Military Modernization and Cross-Strait Balance,' Transcript of the Hearing before the U.S.-China Economic and Security Review Commission. 15 September 2005, https://www.uscc.gov/sites/default/files/transcripts/9.15.05HT.pdf.

Clayton, Mark, 'Ukraine election narrowly avoided 'wanton destruction' from hackers,' Christian Science Monitor, 17 June 2014, http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.

Crawford, Scott, Owen Rogers, Christian Renaud, Carl Brooks, and Adrian Sanabria, 'When things attack: Mirai and the Dyn DDoS attack reveal a disturbing future,' 451 Research, 25 October 2016, https://451research.com/report-short?entityId=90624&referrer=marketing.

Croft, Adrian, and Peter Apps, 'NATO websites hit in cyber attack linked to Crimea tension,' Reuters, 16 March 2014, http://www.reuters.com/article/us-ukraine-nato-idUSBREA2E0T320140316.

Davis, Joshua, 'Hackers Take Down the Most Wired Country in Europe,' Wired, 21 August 2007, https://www.wired.com/2007/08/ff-estonia/.

'DDoS attack halts heating in Finland amidst winter,' Metropolitan.fi, 7 November 2016, http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter.

'DNS Security: Three Ways That Hijacks Can Happen,' Dyn Blog, 28 August 2013, http://dyn.com/blog/dns-101-explaining-how-hijacks-can-happen.

Dwoskin, Elizabeth, 'New Report: Snowden Revelations Hurt U.S. Companies,' The Wall Street Journal, 30 July 2014, http://blogs.wsj.com/digits/2014/07/30/new-report-snowden-revelations-hurt-u-s-companies/.

Etherington, Darrell, 'Amazon AWS S3 outage is breaking things for a lot of websites and apps,' TechCrunch, 28 February 2017, https://techcrunch.com/2017/02/28/amazon-aws-s3-outage-is-breaking-things-for-a-lot-of-websites-and-apps/.

'Executive Order 13636: Improving Critical Infrastructure Cybersecurity,' The Federal Register, 19 February 2013, https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

'Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,' The Federal Register, 11 May 2017, https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

Fox-Brewster, Thomas, 'How Bad Was Cloudbleed? 1.2 Million Leaks Bad,' Forbes, 1 March 2017, https://www.forbes.com/sites/thomasbrewster/2017/03/01/cloudbleed-leak-massive-but-not-too-harmful/#7249ad71613c

Geer, Dan, 'For Good Measure: Stress Analysis,' ;login:, Volume 39, Number 6, USENIX, December 2014, https://www.usenix.org/system/files/login/articles/login_dec14_13_geer.pdf.

Goodin, Dan, 'Massive denial-of-service attack on GitHub tied to Chinese government,' Ars Technica, 31 March 2015, https://arstechnica.com/security/2015/03/massive-denial-of-service-attack-on-github-tied-to-chinese-government.

Goodin, Dan, 'Russian-controlled telecom hijacks financial services' Internet traffic,' Ars Technica, 27 April 2017, https://arstechnica.com/security/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/.

Goodin, Dan, 'Symantec employees fired for issuing rogue HTTPS certificate for Google,' Ars Technica, 21 September 2015, https://arstechnica.com/security/2015/09/symantec-employees-fired-for-issuing-rogue-https-certificate-for-google/.

Grau, Alan, 'IoT Security Standards – Paving the Way For Customer Confidence,' IEEE Standards University, 29 February 2016, http://www.standardsuniversity.org/e-magazine/march-2016/iot-security-standards-paving-the-way-for-customer-confidence.

Greenberg, Andy, 'How Hackers Hijacked a Bank's Entire Online Operation,' Wired, 4 April 2017, https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/.

Greene, Tim, 'How the Dyn DDoS attack unfolded,' Network World, 21 October 2016, http://www.networkworld.com/article/3134057/security/how-the-dyn-ddos-attack-unfolded.html.

'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,' United Nations General Assembly, 22 July 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.

Gurdus, Elizabeth, 'We're headed for a 'cyber Pearl Harbor,' says Adm James Stavridis,' CNBC, 15 December 2016, http://www.cnbc.com/2016/12/15/were-headed-at-a-cyber-pearl-harbor-says-adm-james-stavridis.html.

Harris, Shane, 'Who's Cutting California Internet Cables? The FBI Has No Idea,' The Daily Beast, 4 July 2015, http://www.thedailybeast.com/articles/2015/07/04/who-s-cutting-california-internet-cables-the-fbi-has-no-idea.html.

Hollis, David, 'Cyberwar Case Study: Georgia 2008,' Small Wars Journal, 6 January 2011, www.smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

Huq, Numaan, Stephen Hilt, and Natasha Hellberg, 'US Cities Exposed: Industries and ICS,' TrendMicro, 15 February 2017, https://www.trendmicro.com/content/dam/trendmicro/en/security-intelligence/research/reports/wp-us-cities-exposed-industries-and-ics.pdf.

Hurst, Ryan, 'The foundation of a more secure web,' Google Security Blog, 26 January 2017, https://security.googleblog.com/2017/01/the-foundation-of-more-secure-web.html.

'Inquiry Into Cyber Intrusions Affecting U.S. Transportation Command Contractors,' Report of the Senate Armed Services Committee, 2014. Pp. viii, http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf

'Internet Domain Name and Internet Protocol Address Space Use and Approval,' Department of Defense Instruction Number 8410.01, Department of Defense, issued 4 December 2015, http://www.dtic.mil/whs/directives/corres/pdf/841001p.pdf.

'Internet of Things: Privacy and Security in a Connected World,' FTC Staff Report, Federal Trade Commission, January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

'Iranians hit in email hack attack,' BBC News, 6 September 2011, http://www.bbc.com/news/technology-14802673.

Keranen, Ari, and Carsten Bormann, 'Internet of Things: Standards and Guidance from the IETF,' IETF Journal, Volume 11, Issue 3, April 2016, https://www.internetsociety.org/publications/ietf-journal-april-2016/internet-things-standards-and-guidance-ietf.

Krebs, Brian, 'Akamai on the Record KrebsOnSecurity Attack,' Krebs on Security, 22 November 2016, https://krebsonsecurity.com/2016/11/akamai-on-the-record-krebsonsecurity-attack/.

Lawson, Sean, 'Does 2016 Mark the End of Cyber Pearl Harbor Hysteria?,' Forbes, 7 December 2016, https://www.forbes.com/sites/seanlawson/2016/12/07/does-2016-mark-the-end-of-cyber-pearl-harbor-hysteria/#22c2eac922c2.

Levy, Ian, 'Active Cyber Defence – tackling cyber attacks on the UK,' National Cyber Security Centre Blog, 1 November 2016, https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk.

Marczak, Bill, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, and Vern Paxson, 'China's Great Cannon,' Citizen Lab, 10 April 2015, https://citizenlab.org/2015/04/chinas-great-cannon/.

McConnell, Dugald, 'Report: Chinese company 'hijacked' U.S. web traffic,' CNN, 18 November 2010, http://www.cnn.com/2010/US/11/17/websites.chinese.servers/.

Miles, Donna, 'Transcom, Partners Secure Networks Against Cyberattacks,' American Forces Press Service, Department of Defense, 7 March 2013, http://archive.defense.gov/news/newsarticle.aspx?id=119468.

Miller, Greg, 'Undersea Internet Cables Are Surprisingly Vulnerable,' Wired, 29 October 2015, https://www.wired.com/2015/10/undersea-cable-maps/.

Miller, Rich, 'Challenging Week at 25 Broadway: Telehouse facility wrestles with generator outages, fuel shortages,' CarrierHotels.com, 17 September 2001, http://www.carrierhotels.com/news/September2001/telehouse0917.shtml.

Nordrum, Amy, 'Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated,' IEEE Spectrum, 18 August 2016, http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.

Nordrum, Amy, 'Wanted: Smart Public Policy for Internet of Things Security,' IEEE Spectrum, 10 November 2016, http://spectrum.ieee.org/tech-talk/telecom/security/wanted-smart-public-policy-for-internet-of-things-security.

Perez, Roi, 'Digital Shadows says DDoS extortion on the rise thanks to Mirai botnet,' SC Magazine UK, 14 December 2016, https://www.scmagazineuk.com/digital-shadows-says-ddos-extortion-on-the-rise-thanks-to-mirai-botnet/article/579098/.

Perlroth, Nicole, and Quentin Hardy, 'Bank Hacking Was the Work of Iranians, Officials Say,' The New York Times, 8 January 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

'Project SHINE (Shodan Intelligence Extraction): Findings Report,' Infracritical, 1 October 2014, https://www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014.

'Protecting the Homeland,' Report of the Defense Science Board, 2000 Summer Study, Executive Summary, Volume 1. Pp. 11, http://www.au.af.mil/au/awc/awcgate/dod/dsb_protecting.pdf.

Prudente, Tim, 'Naval Academy reinstates celestial navigation,' Military Times, 1 November 2015, http://www.militarytimes.com/story/military/tech/2015/11/01/naval-academy-reinstates-celestial-navigation/74998554/.

Renz, Bettina, and Hanna Smith, 'Russia and Hybrid Warfare – Going Beyond the Label,' Aleksanteri Papers vol. 1/2016, Kikimora Publications, Aleksanteri Institute, University of Helsinki, Finland. Pp. 44-45, http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf.

Sanger, David E. and Nicole Perlroth, 'A New Era of Internet Attacks Powered by Everyday Devices,' The New York Times, 22 October 2016, https://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html?_r=0/.

Sanger, David E. and Eric Schmitt, 'Russian Ships Near Data Cables Are Too Close for U.S. Comfort,' The New York Times, 25 October 2015, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.

Scola, Nancy, 'Brazil begins laying its own Internet cables to avoid U.S. surveillance,' The Washington Post, 3 November 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/11/03/brazil-begins-laying-its-own-internet-cables-to-avoid-u-s-surveillance/?utm_term=.3f8bd5da0503.

Shamah, David, 'Official: Iran, Hamas conduct cyber-attacks against Israel,' 13 August 2015, http://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/.

Sleevi, Ryan, 'Announcement: Requiring Certificate Transparency in 2017,' Google Groups, 24 October 2016, https://groups.google.com/a/chromium.org/forum/#!msg/ct-policy/78N3SMcqUGw/ykIwHXuqAQAJ.

Sozeri, Efe Kerem, 'Turkish Internet hit with massive DDoS attack,' The Daily Dot, 17 December 2015, https://www.dailydot.com/layer8/turkey-ddos-attack-tk-universities.

'Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends,' International Corporation for Assigned Names and Numbers, 1 October 2016, https://www.icann.org/news/announcement-2016-10-01-en.

'The Department of Defense Cyber Strategy,' Department of Defense, April 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Thomson, Iain, 'You know IoT security is bad when libertarians call for strict regulation,' The Register, 15 February 2017, https://www.theregister.co.uk/2017/02/15/libertarians_call_for_govt_regulation_iot/.

Tikk, Eneken, Kadri Kaska, and Liis Vihul, 'International Cyber Incidents: Legal Considerations, NATO Cooperative Cyber Defence Centre of Excellence, 2010, https://ccdcoe.org/publications/books/legalconsiderations.pdf.

Timberg, Craig, 'The Long Life of a Quick 'Fix'," The Washington Post, 31 May 2015, http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/.

'Usage of SSL certificate authorities for websites,' World Wide Web Technology Surveys, https://w3techs.com/technologies/overview/ssl_certificate/all.

'Using the SIPRNet,' Online Guide to Security Responsibilities, Defense Personnel Security Research Center, Department of Defense, http://www.dhra.mil/perserec/osg/s1class/siprnet.htm.

Vervier, Pierre-Antoine, Olivier Thonnard, and Marc Dacier, 'Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks,' The Network and Distributed System Security Symposium, The Internet Society, 2015, https://www.internetsociety.org/sites/default/files/NDSS2015_Mind_Your_Blocks_Stealthiness_Malicious_BGP_Attacks.pdf.

'Visualizing Global Internet Performance,' Akamai, https://www.akamai.com/us/en/solutions/intelligent-platform/visualizing-akamai/.

Wingfield, Nick, 'Miscue Calls Attention to Amazon's Dominance in Cloud Computing,' The New York Times, 12 March 2017, https://www.nytimes.com/2017/03/12/business/amazon-web-services-outage-cloud-computing-technology.html.

Woolf, Nicky, 'DDoS attack that disrupted internet was largest of its kind in history, experts say,' The Guardian, 26 October 2016, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

Zetter, Kim, 'Someone's Been Siphoning Data Through a Huge Security Hole in the Internet,' Wired, 5 December 2013, https://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/.

Zhou, Liang, and Han-Chieh Chao, 'Multimedia Traffic Security Architecture for the Internet of Things,' IEEE Network, May/June 2011, http://cc.niu.edu.tw/libraryinformation/07-readerserv/essay/04.pdf.

Zwart, Romeo, 'RIPE NCC Authoritative and Secondary DNS services on Monday 14 December,' RIPE Network Coordination Centre, 15 December 2015, https://www.ripe.net/ripe/mail/archives/dns-wg/2015-December/003184.html.

The Cyber Security Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Copyright 2017, President and Fellows of Harvard College

Printed in the United States of America