THE AMERICAN FOREIGN POLICY COUNCIL
Defense Technology Program Brief

October 2015 Washington, D.C. No. 13

Internet Security Governance - Building Security Without Piling On

By Trey Herr and Heather West

Briefing Highlights

Internet Security Governance is the discussion of defensive technical and legal topics that cross national boundaries and/or involve security of the underlying protocols and hardware of the Internet.

• • •

The underlying architecture of the Internet is not secure, but combining and layering new technologies can make it more so.

• • •

Encryption is critical to commerce and secure communications over the Internet. Without it, any information transiting a network would be vulnerable to manipulation or theft by a third party.

• • •

The core protocols of the Internet were developed decades ago, in the 1970s and 1980s. Since 1993, new standards and tweaks to old ones have been formalized and new ones are still needed.

• • •

While the wide variety of stakeholders in the Internet has led to a diverse and economically empowering system of interconnection, it can also inhibit widespread adoption of progressive security measures.

• • •

Imposing a burdensome legal regime on the information security community may seriously harm that community's ability to improve internet security in the U.S. and abroad.

Background Information

Senator Ted Stevens once infamously described the Internet by saying that "it's not a big truck … it's a series of tubes." Though the simplicity of this analogy drew some mockery at the time, there's actually a degree of truth to both parts of it.

Secure web transactions actually can be described as an armored truck moving through a dangerous world. When a web browser makes a secure connection to a web server (e.g., a bank), the packets of information that go between the browser and the server are endowed with cryptographic protections that are like the locks on the truck or the ID card the driver carries – they prevent bad actors from reading the data or impersonating the bank.

The Internet can also be described as a series of tubes. The name is important: The Internet is an "inter-network", a collection of loosely coordinated networks operated by different people. That means that our armored truck driver has to stop and ask for directions as he goes ("Which network is next closest to where I'm going?"). It's also important to make sure that the driver recieves credible directions from the bank, and not a potential bad actor.

Another aphorism useful in cybersecurity is: "If you build it, they will come." The security comunity uses this statement to talk about attacks. An insecure system on the Internet is far more vulnerable to attack, because the barriers to entry are so low. In addition, attackers come in far more guises than those presented by Hollywood. Of course, criminals steal passwords and personal information, but governments collect intelligence and suppres dissent, jealous spouses track financial information, and companies engage in elaborate corporate espionage.

However there's also a more positive sense to the phrase. When two parties make a secure connection over the Internet, they negotiate what security technologies they use. That means that a browser can add support for new technologies (like new encryption methods), and as soon it encounters a web server that also supports that technology, the new and improved protocol will be used. This dynamic can result in very fast changes in the quality of security that gets applied in the Internet. For example, between June 2015 and September 2015, usage of the insecure digital signatures (based on the SHA-1 algorithm) dropped from 70% to 17% of web transactions. This change means that 40 billion transactions a day became more secure.

One final challenge to creating sound Internet policy is the global nature of the Internet. At a technical level, the Internet works the same way everywhere, and companies rely on those correlations to achieve economies of scale and serve a global market. Divergent global policies erode these benefits.

The diversity of goals around the world makes it challenging to set norms around security. When considering Internet policies, it's important to keep a global perspective, both in the sense of establishing consistent global rules that support there being one global Internet, and in the sense of being cautious of how a given policy might apply in a different context.

Background information by Richard Barnes, Firefox Security Lead at Mozilla

Internet Security Governance covers the policy challenges that arise from building and governing security in the Internet's architecture and key protocols. It is not a description of security for computers and networks (Information Assurance),[1] how to manage the negotiated structure and key functions of the Internet (Internet Governance), or the pursuit of criminal groups and other threat actors (Cyber Crime).[2] Internet Security Governance is the discussion of defensively oriented technical and legal topics that cross national boundaries and/or involve security of the underlying protocols and hardware which make up the Internet. These include international agreements, like the Wassenaar Arrangement, and the process of drafting, approving, and promulgating security standards for implementation across the Internet.

Securing the Internet, a fragile network of networks, is a complicated task filled by stopgap solutions that become de-facto permanent out of necessity rather than their provision of ideal security. Perfect security is an impossible dream, owing to the natural fallibility of people responsible for building and implementing secure software as well as the presence of innovative adversaries. Security that is effective for most parties at most times is possible, however. To find a focus amid this vast array of issues, we concentrate on encryption—a process used to establish trust and secure data across networks of every stripe and purpose. To be clear, this is only one of many complex topics in the security environment. Nevertheless, encryption is critical to commerce and secure communications over the Internet. Without it, any information transiting a network would be vulnerable to manipulation or theft by a third party. Using encryption as a focal point, we highlight below several elements of internet security governance; the underlying technology, diversity in national and cultural approaches, and key governance challenges.

Securing the Internet

The Internet is a globally interconnected system of computer networks using shared protocols to facilitate communications between billions of devices, encompassing computers, servers, sensors, and a multitude of other machines. Each of these is connected to a smaller network: a school, a business, a government, or some other public or private entity. While some of these networks are run by a single individual, others are huge intranets maintained by teams of experts.

Each of these local networks is linked by some set of electronic, wireless, or optical networking technology and protocols. Across these links are delivered multiple forms of digital information, from the simple HTML webpage to encrypted email to highly sophisticated applications rivaling anything found on a single computer. The Internet is an all-purposes network of networks connecting diverse arrays of devices and applications, each with different needs but sharing a common dependence on core principles and protocols.

Initially, Internet protocols did not have security elements, as all members of a then-experimental network knew each other and it was more important to create a proof of concept than a complete system. As an early academic network grew into the modern commercial Internet, this lack of security changed—as it had to. Now, there are hundreds of thousands of interconnected networks and billions of connected people, some of them well intentioned, others not.[3] As a result, a global conversation has begun on how best to build security into or on top of the existing protocols of the Internet. A key piece of that security puzzle is the process of encryption.

Encryption

Cryptography affords a measure of security to data in the event it is lost, stolen, or otherwise compromised,

Ms Heather West *works on security, cybersecurity, data governance, and privacy in the digital age at Mozilla, maker of the Firefox browser. She works with stakeholders and policymakers in DC as well as global product and policy teams and was recognized as one of the 2014 Forbes 30 Under 30 in Law and Policy and a Christian Science Monitor Passcode Influencer.* ***Mr. Trey Herr*** *is a senior research associate at the Cyber Security Policy and Research Institute and non-resident fellow with the Cybersecurity Initiative at New America. His work focuses on the relationship between state power and information security including trends in state developed malicious software, the structure of criminal markets for malware, and the regulatory environment for "cyber weapons".*

employing mathematical operations to convert legible information into digital gibberish. The power of these mathematical techniques to obscure data provide a way to secure not only information moving around the internet but also that stored on individual computers and servers around the world.

At any given time, information can be in motion or at rest. Data at rest describes the pictures stored on your phone, the document on a computer, or files backed up on Dropbox. Data in motion is each of these things as they move around the web, along with a bevy of phone calls, tweets, and emails. Encryption provides security against theft or compromise of information and can help guarantee that data hasn't been tampered with, so that you can trust that a message received from someone hasn't been faked by an attacker.

For many years, the only way to encrypt data and share it between parties was through the use of a shared secret, the key. Much as the key to a house is shared if multiple people live there, or else copies made, "symmetric encryption" involves exchanging a shared key between two parties who want to communicate in secret, before they can talk.[4] This runs the risk that an attacker might steal the key and copy it, allowing them to open the encrypted information as well and thus defeating the purpose.

Along came American cryptologists Whit Diffie and Martin Hellman, who, unknowingly extending the work of three British intelligence analysts from the 1970s, developed a way to exchange encrypted data without the use of a shared key.[5] Instead of a single key, Diffie and Hellman's "asymmetric encryption" relies on pair of keys, one public and one private, used by every person who wants to encrypt and securely exchange data. The two keys, linked mathematically, are used to alternately lock and unlock the same file, allowing one person to encrypt a file with the recipient's public key, and send it to be unlocked by the recipient's private key.[6] This way, the public keys could be shared and known to the world while the private keys remained secret, thus solving the challenge of how to exchange a shared key and avoiding the risk someone might steal and copy it. One of the challenges in implementing encryption across different protocols and standards which make up the Internet is the presence of a diversity of stakeholders and networks.

Internet Architecture

Historically, the Internet does not have a centralized method of governance. Instead, each network within the larger Internet (short for internetworking) has the ability set its own policies, while overarching standards are set according to an international multi-stakeholder process, both technical and policy oriented. The layout of these networks is defined not by a handful of global elites but by the networks themselves informally agreeing to interconnect and route traffic between each other. This kind of agreement actually causes the network to be more robust, creating many more potential routes for any given packet to transit, rather than a nationalized or top-down model for routing.

At its highest level, the Internet is a series of Internet Exchange Points (IXPs) joined by radio, copper cable, and fiber-optic links. These represent the physical infrastructure that carries content from Internet Service Providers (ISPs) and Content Delivery Networks (CDNs) and determines where that content is routed between networks.[7] This physical layer is what makes it difficult to argue that the Internet is an entirely new and unregulated space, since the hardware associated with moving bits has to be in or on the ground somewhere. The Internet was designed so that there are many routes traffic can take to get from one point to any other, however; while these IXPs are important, networks do also connect outside of them, so ISPs and CDNs are able to connect directly to each other. These connections are numerous in nature, with major ISPs and CDNs (some companies play both roles) having thousands of formal and informal, paid and unpaid interconnection agreements. This means that even if one route fails, any point should still be reachable by another link or connection.

The underlying architecture of the Internet is not secure, but the possibility of security has been present since its inception owing to flexibility in the way technologies are combined and layered. While a wholesale reengineering is unlikely, there are a number of interim solutions which have been developed, refined, and applied to secure the Internet. The section below details several attempts to design a more secure content delivery and navigation system for the Internet and its users.

Standards and Protocols Evolving for Security

The core protocols of the Internet were developed decades ago, in the 1970s and 1980s. Since 1993, new standards and tweaks to old ones have been formalized through the Internet Engineering Task Force (IETF), a non-profit organization composed of hundreds of technical experts and computer scientists.[8]

Transmission Control Protocol/Internet Protocol: The Backbone

One of many standards adopted and updated by IETF, the Transmission Control Protocol/Internet Protocol (TCP/IP) plays an important role as the backbone of the Internet. Each transaction over the Internet is a series of "packets"—that is, a specifically formatted unit of data that is carried over a series of networks. This packet includes control information, user data, and the "payload"—the actual content or message being carried. TCP/IPs define the standard construction and transmission of these packets.

TCP/IPs were developed and optimized for reliability, not security, so each lacks authentication and encryption capabilities. The security provided to data in motion by encryption is important for a number of reasons, including that it prevents third parties from watching your traffic or manipulating it to, for example, inject it with malware or ads. Changing the protocols themselves presents enormous challenges, so instead, in a pattern replicated across many internet security solutions, another protocol was created to secure the existing one.

Secure Sockets Layer/Transport Layer Security: Securing the Backbone

Enter the secure socket layer (SSL). Netscape Communications created the original SSL in 1994, when it became apparent that there was no way to securely transfer data across the Internet.[9] The first iteration, version 1.0, was so heavily criticized by the security community for using weak cryptographic algorithms that it was never released for public use. As the protocol matured, it became part of IETF's standards-track, engaging the broader technical community in refining and improving it. Through this process, SSL continued to evolve into transport layer security (TLS) in 1999 and through the most recent version, TLS 3.0, which remains in draft form.

The version of IP which has been standard since 1983, IPv4, is slowly being replaced by a new version, IPv6. This updated IP standard has introduced the use of both encryption and cryptographic authentication for all protocols and connections running. The adoption of IPv6 provides a more resilient technical basis than SSL/TLS for secure channels over the insecure Internet. The standard was formalized by IETF in 1998, but the push for adoption, even though recently picking up speed, has generally been slow, with Google finding just under 9% of users accessing their service via IPv6 connections as of September 2015.[10]

Border Gateway Protocol: The Map

The connections between so many different networks over the Internet requires that each must use the same protocols, that is, speak the same language. The typical way of communicating information about how to navigate in and between these networks is the Border Gateway Protocol (BGP). BGP acts as a sort of travel guide to different networks using a distributed database of IP locations, essentially maps of the Internet and subsidiary networks. BGP updates these lists of routes as networks change shape, accepting newly advertised routes from other routers by default.

While an efficient way to map out and navigate the networks, this implicit trust between BGP routers harkens back to the day when all online players knew each other. There is no mechanism of authenticating if routes being offered are legitimate and so raises the risk that routing data could be disrupted or manipulated. This routing information is not encrypted and, as a 2006 memo from the IETF emphasized, "There are no mechanisms internal to BGP that protect against attacks that modify, delete, forge, or replay data, any of which has the potential to disrupt overall network routing behavior."[11] BGP's trust allows for automatic, decentralized, and scalable routing across the Internet's many networks, but also leaves it subject to disruptions by adding or manipulating data in the routing tables.

Securing BGP remains a thorny problem, and while several technical proposals have been put forward, discussion and adoption has been virtually non-existent.[12] Incentivizing change is hard, and many network owners believe the system grants some safety owing to its relatively obscurity and to the fact that their familiarity with each other will help defend against a new, and malicious, user. While the protocol's insecurity looms large, to date the majority of BGP incidents have been failures of capacity and not malicious attacks.[13]

Domain Name Service: The Address Book

The Domain Name System (DNS) system serves as the Internet's address book. If I want to connect to "example.com," where should my packets get sent, and how will they get there? If BGP serves to give computers directions on how to move data across networks, DNS tells them where in the world to go. Every host on the Internet has a range of IP numbers from which their content is served. This system was designed from the outset for usability and robustness, but not for secure and authenticated transactions. While the web is built on DNS, it is a protocol with one major security flaw: there is no guarantee for the end user in DNS that the records received are those sent from the actual source. That means that responses to DNS queries can be forged or manipulated in transit to redirect browsers to connect to a malicious website, add malicious content to a page, or to route email to an attacker's computer.

The importance of DNS as a means of efficiently accessing information and applications on web servers meant this posed a serious challenge. Work began as early as 1995 to create a series of extensions to DNS that would provide authentication for each interaction by encrypting them with a particular key.[14] This process, called DNSSEC, authenticates individual DNS server records first by a central server called the DNS root zone, and then through a chain of trust to pass an authenticated record from the root to child zones and on down to the recipient. Using this chain of trust,[15] DNSSEC can provide authentication of the origin of DNS data, verified confirmation that a DNS entry does not exist, and assurance that the content of the DNS transaction has not been manipulated in transit.

Understanding the Culture(s) of Security Governance

There exists tremendous disagreement between different countries over the question of "what is cybersecurity." More than a cultural gap, these distinctions have taken on tremendous political significance as the range of issues between the United States and countries like China and Russia impede the adoption of useful security standards, the development of norms, and potentially impact the way the Internet is built and operated. Below we highlight several differences between states ranging over issues like law enforcement access to data, stance on encryption, and content filtering.

Russia

Where the U.S. broadly talks about cybersecurity, Russia uses the term Information Security to connote protection from online threats as well as controls on information and interactions that take place online. Both refer to the same protection of architecture, but the Russian phrase also includes law enforcement's ability to retrieve information about individuals and their affairs. This negatively impacts the freedom for firms to offer, or employ as standard, forms of encryption which are not easily compromised in response to government requests. It also supports data localization policies—the requirements that an Internet service firm offering its product in a particular country must also store all user data generated by citizens of that state in the same country. As of this year, Russia requires firms who collect data on Russian users to store that data in servers in Russia.[16] While the law doesn't affect the ability of firms to transfer the data abroad or share it with other companies, it does impose a political requirement, with assoiated technical and legal implications, for all who choose to comply and continue doing business in the country.[17]

China

The Chinese government has several priorities when it comes to the Internet, including the maintenance of economic growth, preserving social stability, supporting ongoing and future military activities, and countering the development of international norms which might undermine any of these goals. This broad swath of activities is covered under the term information security (信息安全, xinxi anquan), while topics like the protection of computers and networks is considered a subset and referred to as network security (网络安全, wangluo anquan).[18] Unlike Russia's focus on data retention and access by agents of the state, Chinese censors have constructed a remarkably flexible arrangement of filtering, blocking, and surveillance technologies, collectively dubbed the Great Firewall of China.[19] The emphasis is on real time monitoring and "shaping" of discussions to control the flow of information from sources outside the country and about sensitive events or phrases within the country.[20] Encryption, especially for data in motion like SSL/TLS, can frustrate these efforts so at different[21] points[22] Chinese officials have used the Great Firewall to block encrypted connections to networks outside of China. While there are a large number of groups with diverse interests as to how Internet security is governed in China, preservation of Chinese Communist Party (CCP) influence and political stability appear to be of paramount importance.[23]

United States

The United States has been home to much of the innovation and commercial development which brought about the Internet's arrangement of protocols, hardware, and security standards as we know it today. Part of the challenge in governing this array of issues has been for the United States to work with countries that may be suspect of being—or outwardly hostile to—this predominance. While support for an open and secure Internet is rhetorically part of U.S. policies,[24] attempts to undermine security standards[25] and the availability of strong encryption tools[26] has provided evidence to some who doubt the sincerity of such a narrative. Existing domestic legal protections for free speech have provided a bulwark[27] against censorship and domestic content filtering, but concerns over law enforcement access to data, especially abroad, has generated proposals which may compromise security.[28]

The Practice of Governing Internet Security

A network of responsibilities governs the technical architecture of the Internet across national and cultural boundaries. In some cases, these functions are fulfilled by public institutions and clear statutory mandates, while others are handled by private companies and informal arrangements. A serious challenge to the collective governance of internet security is the array of private owners and non-governmental standards bodies whose coordination has yielded a diverse and economically empowering system of interconnection and commerce, but whose variegated nature and diverse incentives can inhibit widespread adoption of progressive security measures.

Here, we describe three major examples of this governance environment. Each impacts a different facet of interstate cooperation and technical coordination. Certificate Authorities govern the trust network that underpins encryption for data in motion, including the SSL/TLS protocols. MLAT or Mutual Legal Assistance Treaties govern the cooperative investigation and coordinated prosecution of criminals across jurisdictions. The Wassenaar Arrangement is an example of multilateral cooperation to attempt to establish and enforce standards to improve internet security.

The Certificate Authorities System

Certificate Authorities (CAs) act to certify that internet services using SSL/TLS encryption are communicating in secret and are who they claim to be. The CAs system is the network of companies and, in some cases non-profit groups, that issues, signs, and publicly shares digital certificates to certify the owner of a public key (the internet service) by issuing a certificate signed with their private key (the CA). CAs are one of the central trust mechanisms on the Internet so any vulnerabilities at the CA level impact a significant portion of the Internet's data in motion that is presumed to be secure. These Certificate Authorities figure prominently in the setup of the Public Key Infrastructure (PKI) implementation on the Internet, providing the trusted entity that can authenticate interactions for secure exchange of content. Based on this authentication, browsers and servers can negotiate a symmetric key (as opposed to the asymmetric key used for the certificate authenticating the exchange) to ensure that the content exchanged is safe from both prying eyes and manipulation by malicious third parties.

This PKI system has become a truly distributed and global trust mechanism. Each browser manufacturer decides which CAs it considers trusted, and includes a list with the browser (and likely includes the option to add more CAs, such as a self-signed CA for an internal network). Because of the role serves as a trusted list of certificate, a CA compromise means that the communication is no longer provably secure. In July of 2011, a CA called DigiNotar released a fraudulent certificate for Google that Iranian intelligence services used to intercept information from more than 300,000 Google Mail users.[29] Investigations into the breach revealed that previous hacks had used DigiNotar to issue dozens of certificates for Yahoo, Mozilla, and Tor, among others. Once discovered, the certificates associated with the DigiNotar breach were recognized and quickly revoked across all major browsers. This incident is only one of several that have impacted the CA system, underlining the need for a flexible network of firms and non-profit groups able to respond rapidly to security threats and compromise.

Law Enforcement: Clarifying Cooperation

MLATs or Mutual Legal Assistance Treaties, are a mechanism for countries to share information related to ongoing investigations in circumstances where foreign assistance is necessary for a domestic prosecution. They provide a legal basis for international law enforcement activity like extradition and the seizure of assets.[30] As crime related to information technology has become a more substantial part of the legal landscape, the language of these documents has struggled to keep up. A key issue is most MLATs have limited or non-existent provisions for balancing privacy protections against government interest in data and distinguishing between content and metadata in shared information.[31]

These sort of ambiguities can impede cooperation between countries whose legal systems differ in their privacy protections. It also imposes a burden on an already limited Federal organizational capacity to understand the validity of requests for information and respond appropriately within the framework of U.S. law. The President's Review Group on Intelligence and Communications Technologies found that requests "appear to average approximately 10 months to fulfill, with some requests taking considerably longer. Non-U.S. governments seeking such records can face a frustrating delay in conducting legitimate investigations."[32] The effect of this is to dissuade the use of MLATs as a means to exchange data between law enforcement groups and prosecutors. And yet, providing a clear and responsive channel for international legal information requests is precisely what the MLATs are intended for.

Improving the MLAT process should start with reducing the cost associated with each request to other governments and to U.S. law enforcement bodies by creating a secure digital means to submit and update requests. It should also include reform of the language found in existing agreements, with several goals in mind. First, to clarify the balance of privacy expectations against government interest in information, and to introduce technically significant distinctions such as the one between the content of communications and the metadata related to their address and routing. Second, to set clear expectations of what the United States will and will not turn over. As a jurisdiction which covers a substantial number of data storage and Internet communications services, American firms will be a popular target for data requests from the security and law enforcement services of other countries. A clearly structured and responsive process will help attenuate (although not remove) the incentive for foreign governments to put into place extraordinary requirements like data localization and dissuade other more exotic and costly legal mechanisms.

Regulating Security Away

One of the vehicles pursued by states in trying to structure the security environment are export controls targeting malicious software components. The Wassenaar arrangement is an international export control regime brought into force in 1996 to cover sophisticated military and dual use technologies including jet engines and advanced sensors.[33] The arrangement does not constitute new law in and of itself. Rather, it is a standing mechanism to define common expectations among states and basis on which to harmonize different domestic laws.[34] In 2013, the Arrangement was edited to cover technologies like deep packet inspection tools and "intrusion software"—malicious software designed to extract or modify data and system processes.[35] Part of the intent behind the change, proposed the French and British governments,[36] was to deter the sale of surveillance software and technologies to repressive regimes.

But the resulting changes, as well as the subsequent rule proposed by the U.S. Department of Commerce to harmonize American law with the Arrangement, were written such that they cover both these surveillance products as well as a range of defensive tools and information. These include software used for penetration testing by defensive security firms like Metasploit, the popular framework developed by H.D. Moore and now maintained by Boston-based information security company Rapid7. More problematically, although there is some disagreement on this score between the Commerce Department's Bureau of Industry and Security and most outside analysts, the proposed rules do appear to also cover exploits, the code which takes advantage of a flaw or feature in software to allow unintended operations by a third party. Exploits are bought and sold by numerous groups, both malicious and well intentioned, but their free flow and exchange plays a significant role in major software vendor's information security strategy.

There are serious challenges in using export controls as a means to govern internet security, especially when focusing on software code, for which there exists an overwhelming variety of means to exchange ideas and tools across borders. Leveraging a set of regulations whose original intent was to restrict the flow of things like missile guidance systems and avionics, and using U.S. laws which also cover the sale of nuclear energy components and firearms unnecessarily equates a great deal of information security research with deviant behavior. More importantly, the imposition of a large and complicated legal regime on the information security community, the value of which has come in great part from the agility to coordinate and collaborate in unexpected ways, may seriously harm efforts to improve internet security in the United States and abroad. A clear path forward to undoing the harm threatened by the proposed changes to U.S. law[37] is to pause the Department of Commerce's rulemaking process until the Wassenaar Arrangement language can be further amended in the next plenary session (slated to take place in either February 2016 or 2017). Modifications should remove the language which might cover exploits, exploit techniques, and legitimate vendor updating and security services.[38]

Where Do We Go From Here?

Internet Security Governance covers those security topics that are defensive in nature (e.g., not related to the active interdiction of threats) and are multilateral and/or international in scope. This includes formal interstate relations like the Wassenaar Arrangement and MLAT process, as well as private sector led efforts like the network of certificate authorities underpinning encrypted communications on the web. While the focus of these issues involves global standards, the influence of diverse national value systems and approaches to the topic cannot be underestimated.

Perhaps the most challenging realization is the sheer diversity of stakeholders and priorities involved with the development and adoption of security standards. This process has generated tremendous technical achievements but somewhat fragile institutions, whose operation is necessary to a secure and functioning internet. The recommendations contained here are a starting point: to reform the MLAT process to lower response times and clarify expectations and treatment of digital information, modify the language of and deemphasize export control regulations as a means of controlling security products, and to help industry and technologists reinforce the security of the Certificate Authorities system, maintaining the flexibility and responsiveness of private ownership. Improvement, it seems, should come carefully and be rooted in the same non-state organizations and private actors who have been largely responsible for the Internet's achievements thus far.

Endnotes

1) Herr, Trey and Eric Ormes, "Understanding Cybersecurity – Part 2 - Information Assurance," American Foreign Policy Council, April 15, 2015. http://www.afpc.org/publication_listings/viewPolicyPaper/2754
2) Herr, Trey and Sasha Romanosky, "Cyber Crime: Security Under Scarce Resources," American Foreign Policy Council, June 30, 2015. http://www.afpc.org/publication_listings/viewPolicyPaper/2827
3) "Number of Internet Users," Internet Live Stats. http://www.internetlivestats.com/internet-users/
4) Simmer, David, "Crypto Primer," March 14, 2014. https://www.davidsimner.me.uk/2014/03/crypto-primer
5) "GCHQ Trio Recognized for Key to Secure Shopping Online," BBC, October 4, 2010. http://www.bbc.com/news/uk-england-gloucestershire-11475101
6) Palmgren, Keith, "Diffie-Hellman Key Exchange – A Non-Mathematician's Explanation," SecurityPortal, August 22, 2006.
7) "Global Traffic Map 2010," TeleGeography. https://www.telegeography.com/assets/website/images/maps/global-traffic-map-2010/global-traffic-map-2010-x.jpg
8) Cerf, Vint, "IETF and the Internet Society," Internet Society, July 18, 1995. http://www.internetsociety.org/internet/what-internet/history-internet/ietf-and-internet-society
9) Freier, A. et. al., "The Secure Sockets Layer (SSL) Protocol Version 3.0," Internet Engineering Task Force, August 2011. https://tools.ietf.org/html/rfc6101
10) "IPv6 Adoption," Google Statistics. http://www.google.com/intl/en/ipv6/statistics.html
11) Murphy, S., "BGP Security Vulnerabilities Analysis," Network Working Group, January 2006. http://www.ietf.org/rfc/rfc4272.txt
12) Alaettinoglu, Cengiz, "BGP Security: No Quick Fix," Network Computing, February 26, 2015. http://www.networkcomputing.com/networking/bgp-security-no-quick-fix/a/d-id/1319235
13) Anthony, Sebastian, "Brace for the BGPocalpse: Big disruptions loom as internet overgrowth continues," ExtremeTech, August 13, 2014. http://www.extremetech.com/extreme/187954-brace-for-the-bgpocalypse-big-disruptions-loom-as-internet-overgrowth-continues
14) Bellovin, Steven, "Using the Domain Name System for System Break-ins," AT&T Bell Laboratories, June 1995. http://www.cse.iitd.ernet.in/~sbansal/csl865/readings/bellovin.pdf
15) Sullivan, Nick, "DNSSEC: An Introduction," CloudFlare, October 07, 2014. https://blog.cloudflare.com/dnssec-an-introduction/
16) Amos, Howard, "Apple to Store Users' Personal Data in Russia," The Moscow Times, September 10, 2015. http://www.themoscowtimes.com/business/article/apple-to-store-users-personal-data-in-russiareport/529865.html
17) Blagov, Sergei, "Russia Clarifies Looming Data Localization Law," BNA, August 10, 2015. http://www.bna.com/russia-clarifies-looming-n17179934521/
18) Amy Chang - "Warring State: China's Cybersecurity Strategy" - http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang_report_010615.pdf
19) Barme, Geremie and Sang Ye, "The Great Firewall of China," Wired, June 01, 1997. http://archive.wired.com/wired/archive/5.06/china.html
20) Zittrain, Jonathan and Benjamin Edelman, "Empirical Analysis of Internet Filtering in China, Harvard Law School, March 20, 2003. http://cyber.law.harvard.edu/filtering/china/
21) Arthur, Charles, "Chine Tightens 'Great Firewall' Internet Control with New Technology," The Guardian, December 14, 2012. http://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control
22) "China Blocks Virtual Private Network Use," BBC. January 26, 2015. http://www.bbc.com/news/technology-30982198
23) Chang, Amy, "Warring State: China's Cybersecurity Strategy," CNAS, December 2014. http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang_report_010615.pdf
24) Kerry, John, "An Open and Secure Internet: We Must Have Both," US State Department, May 18, 2015. http://www.state.gov/secretary/remarks/2015/05/242553.htm
25) Green, Matthew, "A Few Thoughts on Cryptographic Engineering," January 14, 2015. http://blog.cryptographyengineering.com/2015/01/hopefully-last-post-ill-ever-write-on.html
26) Wilson, Andi et al., "Doomed to Repeat History? Lessons From the Crypto Wars of the 1990s," New America, June 17, 2015. https://www.newamerica.org/new-america/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/
27) "First Amendment Rights and the Internet," NEA, September 1997. http://www.nea.org/assets/docs/HE/vol3no3.pdf
28) Wagstaff, Keith, "FBI Director Says Encryption Poses Law Enforcement Challenge," CNBC, July 08, 2015. http://www.cnbc.com/2015/07/08/fbi-director-says-encryption-poses-law-enforcement-challenge.html
29) Fisher, Dennis, "Final Report on Diginotar Hack Shows Total Compromise of CA Servers," Threat Post, October 31, 2012. https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/
30) Kendall, Virginia and Markus Funk, "The Role of Mutual Legal Assistance Treaties in Obtaining Foreign Evidence," Litigation, Volume 40, Number 2, Winter 2014 http://www.americanbar.org/content/dam/aba/events/criminal_justice/CSR_MLAT_LetterRogatory.authcheckdam.pdf
31) Hill, Jonah, "Problematic Alternatives: MLAT Reform for the Digital Age," Harvard Law School National Security Journal, January

28, 2015. http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/

32) “Report and Recommendations of the President’s Review Group on Intelligence and Communications Technologies,” December 12, 2013, pg. 227. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

33) “Genesis of the Wassenaar Arrangement,” http://www.wassenaar.org/introduction/print_origins.html

34) “Export Controls for Conventional Arms and Dual-Use Goods and Technologies,” Wassenaar Arrangement, January 2012. http://www.wassenaar.org/publicdocuments/2012/Basic%20Documents%202012.pdf

35) Granick, Jennifer, “Changes to Export Control Arrangement Apply to Computer Exploits and More,” Stanford Law School Center for Internet and Society, January 15, 2014. http://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more

36) “Comments to the US Department of Commerce on Implementation of 2013 Wassenaar Arrangement Plenary Agreements,” CNS, July 20, 2015. https://cdt.org/files/2015/07/JointWassenaarComments-FINAL.pdf p.2

37) Varmazis, Maria, “Availability of Metasploit Community & Metasploit Pro trials outside US and Canada,” Rapid7Community, June 05, 2015. https://community.rapid7.com/community/metasploit/blog/2015/06/05/availability-of-metasploit-community-metasploit-pro-trials-outside-us-canada

38) Herr, Trey and Paul Rosenzwieg, “Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model” Journal of National Security Law and Policy, October 23, 2015. http://jnslp.com/2015/10/23/cyber-weapons-export-control-incorporating-dual-use-with-the-prep-model/

Defense Technology Program Brief

About The Defense Technology Program

A revolution is taking place in the nature of warfare. The proliferation of ballistic missiles and weapons of mass destruction has given rogue states and terrorist groups unprecedented access to potentially devastating capabilities, while space and cyberspace have emerged as distinct new arenas of strategic competition. The American Foreign Policy Council's (AFPC) work in these areas is aimed at helping U.S. offcials understand and respond to this new, and increasingly complex, threat environment.

For more information about the program, please contact Richard Harrison, Director of Operations and Defense Technology Programs at harrison@afpc.org.

About AFPC

For over three decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

AFPC Mission Statement

The American Foreign Policy Council seeks to advance the security and prosperity of the United States by:

- providing primary source information, as well as policy options, to persons and organizations who make or influence the national security and foreign policies of the United States;
- arranging meetings and facilitating dialogue between American Statesmen and their counterparts in other countries; and
- fostering the acceptance and development of representative institutions and free market economies throughout the world in a manner consistent with the Constitution, the national interest, and the values of the United States.

AFPC STAFF

Mr. Herman Pirchner, Jr.
President
Mr. Ilan Berman
Vice President
Mrs. Annie Swingen
Director for External Relations
Mr. Jeff M. Smith
Director of Asian Security Programs and Kraemer Strategy Fellow
Mr. Richard Harrison
Director of Operations and Defense Technology Programs
Ms. Amanda Azinheira
Research Fellow and Program Officer

BOARD OF ADVISORS

Amb. Paula J. Dobriansky
Hon. Newt Gingrich
Amb. Robert G. Joseph
Sen. Robert Kasten, Jr.
Amb. Richard McCormack
Hon. Robert "Bud" C. McFarlane
Gov. Tom Ridge
Dr. William Schneider, Jr.
Hon. R. James Woolsey
Hon. Dov Zakheim

CONTACT

509 C Street NE
Washington, D.C. 20002
Telephone: 202.543.1006
Fax: 202.543.1007
www.afpc.org