ITIF
The Information Technology & Innovation Foundation

How to Stop the Billions Wasted Annually On Email Spam

BY DANIEL CASTRO | JULY 2013

Spam is a worldwide concern, wasting valuable network bandwidth, lowering productivity, and costing businesses and consumers billions of dollars per year. Moreover, it is the symptom of a much larger disease—a flourishing underground Internet economy evolving to meet the needs of cybercriminals.

On May 1, 1978, an employee at Digital Equipment Corporation (DEC) sent out a message advertising demos of the DECSYSTEM-20 mainframe computer to all the users listed in the ARPANET directory.[1] Users reacted swiftly and negatively to this unsolicited message, and rightfully so since at that time ARPANET, the precursor to the Internet, was intended to be used for official U.S. business only. Since then, the problem of widely-distributed, unsolicited, commercial email messages has grown into a worldwide concern, wasting valuable network bandwidth, lowering productivity, and costing businesses and consumers billions of dollars per year. While there have been many attempts at technical and policy solutions, thirty-five years later spam still remains an ever-present problem on the Internet. Moreover, spam is the symptom of a much larger disease—a flourishing underground Internet economy evolving to meet the needs of cybercriminals.

This report outlines the scope of the spam problem today, the challenges of stopping it, and recommendations for additional steps policymakers can take to combat spam and related cybersecurity challenges. These recommendations include:

- Recognize spam as one part of the larger cybersecurity problem and develop and deploy comprehensive cybersecurity countermeasures, including best practices in the private sector to a) increase the use of effective anti-spam technology, b)

combat botnets and bulletproof hosting, and c) reduce misuse of affiliate marketing programs
- Increase resources for enforcement actions against cybercriminals, especially those engaging in practices that facilitate spam or otherwise harm consumers and businesses
- Support international efforts to combat spam, including by adding strong cybersecurity measures to trade agreements
- Implement a "name and shame" program to discourage legitimate companies from providing services to spammers and other cybercriminals

WHAT IS THE SCOPE OF THE PROBLEM?

As the number of Internet users has grown, so too has the amount of email spam. At its peak in June 2010, there were approximately 340 billion spam messages sent daily, which accounted for 90 percent of all email traffic.[2] The total amount of spam worldwide has declined substantially since then, mainly a result of law enforcement efforts, but it still remains high. The amount of spam on the Internet fluctuates from month to month. In the eighteen month period between January 2012 and June 2013, worldwide spam was at its highest in March 2013 with 151 billion daily spam messages, and at its lowest in January 2012 with 74 billion spam messages.[3]

Figure 1: Average daily volume of spam messages worldwide in billions, June 2009 – June 2013.[4]

The vast majority of spam is sent by botnets: networks of computers infected with malware that allow an attacker to control them.[5] In general, countries with a significant online presence are more likely to be the source of spam because they are more likely to have compromised computers. The exact rankings change over time and vary based on who

tracks spam, but there are some consistent offenders. According to the computer security firm Trend Micro, in 2012 the top five countries for sending spam were India, Saudi Arabia, the United States, South Korea, and Peru.[6] Together, these five countries produced approximately one-third of the worldwide spam. Another security company, SophosLabs, reported that the top spam sending countries in 2012 were India, the United States, Italy, South Korea, and Brazil.[7] These rankings do not mean that the spammers themselves were based in these countries; only that they used computers in these countries, often illicitly, to send spam.

While spam is difficult to prevent, technical measures to block it from consumers have been highly successful.[8] Commercial email service providers, including ISPs and web-based email services, have minimized the amount of spam that users see in their inboxes.[9] As of 2012, the vast majority of webmail users (over 855 million worldwide) used three main providers: Google Gmail, Microsoft Hotmail, or Yahoo Mail. These services have invested heavily in anti-spam technology. Using insights gained from processing such a significant percentage of global email they are able to provide low-cost and highly-effective filtering for a large segment of Internet users.[10] For example, the anti-spam costs for Yahoo Mail are only $0.10 per user per year.[11] These webmail services also benefit from crowd-sourced data: if many users flag a message as spam, the cloud-based anti-spam filters can learn in real-time and protect other users.

The experience of business email users depends on the types of spam filters used by an organization. In recent tests of commercial spam filters, most products blocked more than 99 percent of spam email and had a low false-positive rate.[12] Still, no email filter is perfect, and some spam gets through, even as some legitimate email gets incorrectly flagged as spam. This wastes time for users and results in users not receiving some legitimate messages.[13] In addition, not all users or organizations choose email services with good spam filters, so user experience with spam varies.

Surveys provide some insight into how users experience spam. In a series of 2011 surveys of U.S. Facebook and Google users, Gallup and *USA Today* found that slightly more than half were "not too concerned" or "not concerned at all" about spam; slightly less than half were "very concerned" or "somewhat concerned."[14] An earlier survey in 2007 (when the average daily spam was around current levels) found that 18 percent of U.S. adults thought "spam is a big problem" (down from 25 percent in 2003), whereas 51 percent reported that "spam is annoying, but not a big problem" and 28 percent said "spam is not a problem at all."[15] User surveys can be a poor indicator of the scope of the illegal spam problem discussed in this report, since users do not necessarily distinguish between merely unwanted email messages (e.g., legal direct marketing, newsletter subscriptions, account statements and notices, jokes from friends, etc.) and illegal "spam" (i.e., unsolicited bulk commercial email). Many users receive legal direct email marketing from businesses. For example, users may sign up to receive emails from retailers after making a purchase. Sometimes users do this inadvertently, forget they signed up, or later change their minds. But because the users may not want these messages or find them to be a nuisance, users may consider these messages to be spam too when responding to surveys. In addition, although users can

unsubscribe from annoying emails, they may be concerned about the security risks of clicking the necessary links and avoid doing so.

While advances in anti-spam technology help protect consumers from seeing the majority of the spam that is sent, there are still significant negative externalities from spam.[16] There have only been a few attempts at quantifying the total financial cost of spam for businesses and consumers, and none of the methodologies is perfect. Ferris Research, a U.S.-based market research firm, estimated that in 2005 the total global cost of spam for businesses was $50 billion and the cost for the United States alone was $17 billion.[17] The study focused on three costs: productivity costs, help-desk costs (to deal with spam-related problems), and anti-spam technology costs. The productivity costs were based on estimates of the time wasted inspecting and deleting spam that is not caught by filters and searching for legitimate email that was deleted erroneously by filters. The costs of additional server capacity or bandwidth to handle spam messages were not included in this estimate. Nor were other direct costs, such as fraud, theft, security breaches, and lost business; or indirect costs, such as a loss of consumer trust in a brand or the Internet. Spam can also mask more nefarious spear phishing attacks, where attackers, especially foreign adversaries or competitors, use email spoofing to target specific individuals or organizations to gain access to sensitive information, including trade secrets and other intellectual property of U.S. firms.[18] The Ferris Research study did not include email accounts that were used for personal use in its estimate. The firm updated its study in 2009, when spam volume was near its historical peak. The global cost of spam at this time was estimated to be $130 billion, with the U.S. share being $42 billion (or approximately $317 per year per U.S. household).[19]

A more recent study in 2012, co-authored by security researchers at Microsoft Research and Google, used a similar methodology but different data sources to assess the total cost of spam for users in the United States. They estimated the total cost of spam to be between $18 and $26 billion. This study's lower estimate in part reflects the authors' assumption that the percent of spam that evades anti-spam technology and reaches users is lower than estimated by Ferris Research. (The former estimate the percent of spam unsuccessfully caught to be between 1.8 to 3 percent; the latter estimate 5 percent.[20]) Despite discrepancies, these estimates show that the economic cost of spam is significant and consequential. And the estimates would be even higher were it not for existing spam mitigation efforts by the private sector.

Spam continues to be a problem because it is profitable for those sending it. The 2012 study discussed above estimates that all together spammers earn $200 million per year.[21] Using the more recent estimates of the cost of spam, this means that for approximately every dollar that spammers earn in revenue, they cost businesses and consumers $90 to $130.

Spammers use different "business models" to earn revenue from spam, including the following:

- Illicit goods: Spam is used to advertise illicit goods and services, such as pharmaceuticals from black market pharmacies, online casinos, and counterfeit products, such as fake luxury goods and software.
- Affiliate programs: Spam is used to send users to legitimate websites that pay for customer referrals. While legitimate businesses may have affiliate programs that prohibit the use of spam for referrals, in practice it is difficult to enforce.
- Marketing: Spam is used to advertise products and services from legitimate businesses that use illegitimate marketing practices, either knowingly or unknowingly, such as mortgages and loans and adult websites.
- Scams: Spam is used to propagate scams, such as the infamous Nigerian scams, work-at-home scams, dating site scams, pump and dump schemes (where spammers try to inflate the price of microcap stocks), and pyramid schemes.[22]
- Malware: Spam is used to distribute viruses and other malware through email messages. Some spammers earn revenue through pay-per-install affiliate programs whereby other cybercriminals pay spammers for every user who is tricked into installing malware on his or her computer. For example, a botnet operator might pay a bounty for every new infected PC.[23]
- Phishing: Spam can also be used as part of a phishing attack to steal usernames, passwords, and credit card information. Users may be misled into installing software on their PCs that collects this information; or users may be tricked into entering private information on an illegitimate website.
- Propaganda and other information: Spam is used to circulate ideas and information, including content that may not be legally distributed through other channels, such as pornography, propaganda, and hate speech. For example, spammers may try to influence an election. Spam should not be confused with legal email marketing that users have opted-in to receive.

Spammers constantly change their techniques to get users to open their email messages. They might use low-priced drug offers, lonely hearts ads, and counterfeit messages, such as fake email delivery failure notices. Spam may also be seasonal, with spammers sending messages advertising discounted flowers before Mother's Day or special deals on cigars before Father's Day.[24] Often spammers will impersonate legitimate businesses to lend credibility to their email messages, such as by usurping the name of a well-known company or product. These messages are particularly harmful since they hurt the brands of legitimate companies and promote consumer distrust. For example, spammers have used emails that mimic delivery notifications from shipping companies like UPS and FedEx.

In addition to email, spam is also a growing problem on websites, such as blogs and forums, instant messaging services, and social networks like Facebook and Twitter. Spammers post messages on these websites and networks to advertise services, increase

search engine rankings, and lure Internet users to compromised websites. For example, in September 2012, spammers took over many user accounts on Pinterest which resulted in image spam on a variety of social media networks to which users have their accounts linked, such as Facebook and Twitter. In this case, the spam was intended to get users to participate in a work-at-home program.[25] Spam on these sites decreases the value of these websites for users and lowers productivity, as manual labor must be spent moderating messages to eliminate spam. Finally, SMS spam is a growing problem. In 2013, the Federal Trade Commission (FTC) charged twenty-nine individuals with sending 180 million spam text messages to consumers, most falsely advertising free gift cards to retailers or free electronics.[26] As shown in Figure 2, a 2012 Pew Internet & American Life Survey found that among U.S. adults who text message on their cell phones, 25 percent receive SMS spam at least weekly.[27] In some cases, the recipients must pay for the SMS spam they receive. While SMS spam is a problem, its volume is relatively low in the United States compared to other countries like China, in part because the cost of sending SMS messages is significantly higher in the United States than some other countries.[28] Some spammers try to avoid this restriction by using phones infected with malware to send unauthorized text messages.[29]

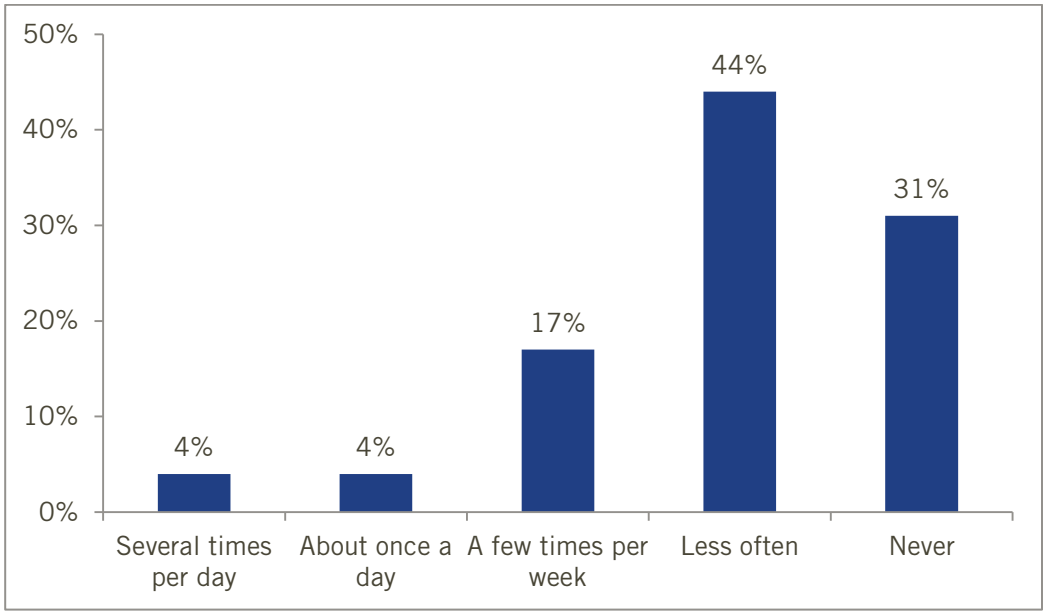

Figure 2: Incidence of spam among adult U.S. cell phone owners who text.[30]

WHAT HAS ALREADY BEEN DONE?

Both technical and political solutions have been deployed to address spam. The two primary technical countermeasures to spam are automated filters and access control lists such as blacklists and whitelists. Automated software-based filters identify email as potential spam using a combination of techniques, including rule-based filtering, i.e., filtering out email that matches certain keywords or that contains certain subject lines; and statistical classification, most commonly Bayesian filtering. Software filters can also help protect users from receiving forged emails from spammers by matching the sender's IP address to a domain name system (DNS) entry or using other forms of domain-based email

authentication (e.g., Sender Policy Framework or DomainKeys Identified Mail). Email service providers use black lists to block certain known offenders or white lists to allow only approved senders to send email to a specific mail server. Black lists and white lists can be used based on specific domains or specific IP addresses. Technical measures to block spam are highly effective, in part because widely deployed anti-spam technologies analyze such a large corpus of email. Hence, once a message is identified as spam it can be classified as such for all users.

On the policy side, a number of countries have passed laws to combat spam. While many countries are interested in protecting free speech, the standard is typically lower for commercial speech. Thus, some anti-spam laws define spam as "unsolicited commercial email" (i.e., email that is widely-distributed, unsolicited, and commercial) whereas others define it as "unsolicited bulk email" (i.e., email that is widely-distributed and unsolicited but that can be either commercial or non-commercial). Using the former definition, some non-commercial email, such as political messages, would not fall under some anti-spam laws. In Europe, some countries such as Austria prohibit unsolicited bulk email, while others, such as Germany, Italy, and Finland prohibit unsolicited commercial email. The African Union Commission (AUC) has developed jointly with the United Nations Economic Commission for Africa (UNECA) a convention on cyber legislation. Included within this convention is a ban on direct marketing (including email, fax, etc.) without the prior consent of the individual recipient and without providing contact information for individuals to unsubscribe.[31]

In the United States, the government has more leeway in regulating commercial speech than non-commercial speech, such as political messages, as the latter may be protected under the First Amendment. The federal CAN-SPAM Act, passed in 2003, regulates commercial email at the federal level by requiring that senders abide by certain conditions, such as not using false header information or deceptive subject lines, identifying messages as an advertisement, providing a valid physical contact address for the sender, telling consumers how to opt out of future emails, and honoring opt-out requests. The law also established civil and criminal penalties for spammers, especially for egregious violations. This law has had two main benefits. First, it has standardized the direct marketing email practices of law-abiding businesses and enabled consumers to opt out of emails. Second, it has allowed law enforcement officials to take action against some domestic spammers. A related bill, the Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 (U.S. SAFE WEB Act,) gave the FTC new authority to pursue investigations and enforcement proceedings, especially for cross-border cases.[32]

In addition, most states have their own state-level anti-spam laws which allow state law enforcement officials to take action against spammers.[33] Not all of these laws have been successful, especially those that include non-commercial bulk email. For example, in 2004 the Commonwealth of Virginia convicted Jeremy Jaynes, of sending spam. At the time Jaynes was the eighth-most-prolific spammer in the world, and was earning between $500,000 and $750,000 per month through spam.[34] The state sentenced him to nine years in jail, but the state Supreme Court eventually overturned his conviction because it ruled that the state's anti-spam law was too broad and violated the right to free speech.[35]

Various international organizations work together to address spam issues. Chief among these are the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) and Spamhaus. M3AAWG is a global industry-supported organization focused on improving online safety for consumers and reducing abuse of messaging systems. M3AAWG promotes industry collaboration with academics and governments, works to improve anti-spam technology, and advises on policy issues. It has also issued a series of voluntary best practices, such as recommendations for ISPs on how to address botnets. Spamhaus is an international non-profit organization formed in 1998 to track spam operations, provide anti-spam countermeasures, and lobby for more effective anti-spam legislation. In particular, Spamhaus is known for maintaining, and making freely available to the public, a series of blacklists to block spam and malware on the Internet. Spamhaus also tracks known spam operations to help service providers avoid business with known cybercriminals.[36] Finally, Spamhaus maintains a list of ISPs that do the least to respond to abuses.[37]

WHY IS SPAM HARD TO PREVENT?

There are many reasons why spam is difficult to prevent. From the technology side, the email protocol, Simple Mail Transfer Protocol (SMTP), was designed to allow any sender to push out a message to any recipient, much like postal mail, text messages, and faxes. Also, like many of these systems, the sender is not authenticated so messages may be sent anonymously or from falsified addresses. Thus the email system is inherently insecure, and while there are alternative messaging platforms such as social media sites, none have the same reach as traditional email.

Spammers are in a constant arms race to defeat anti-spam technologies. In response to early keyword blocking, spammers used alternative spelling like "V1agra" instead of "Viagra"; in response to more advanced filters, spammers began displaying images in emails to avoid textual analysis. In response to anti-virus software that detects malware on sites spammers send to users, spammers have begun using server-side polymorphism so that the malicious code changes and regenerates every few minutes to make it more difficult to detect.[38] In addition, a number of more recent innovations have made it easier for spammers to send unsolicited email, including botnets, fast-flux DNS, and bulletproof hosting, as described below.

Botnets are networks of computers infected with software that allows a central computer to control them. Botnets can range in size, but the larger ones can contain hundreds of thousands of computers. Each infected computer in a botnet can send a substantial amount of spam. This means that a criminal in control of a botnet with a million computers can send spam from one million different IP addresses. Or a spammer can use a botnet and stolen credentials to send spam through other mail servers while masking the source. Computer that were part of the Waledac botnet were capable of sending out 2,000 spam emails per hour.[39] The use of botnets makes it difficult for anti-spam software to block spam on the basis of IP addresses and for law enforcement officials to investigate spam.

Botnets use various techniques to avoid detection. For example, secondary relay nodes can protect all of the infected machines in the botnet from being enumerated. And botnets are

constantly evolving to evade new security countermeasures. The Asprox botnet has been around since 2007 and has added new features to avoid detection and remain effective. This botnet allows the software on infected computers to be updated, uses encryption to secure its communication to the command and control servers to avoid being detected at the network-level, and constantly scans for compromised legitimate websites so it can further distribute malware without detection.[40] Botnets also use a technique called fast-flux DNS to get around anti-spam efforts. Fast-flux DNS resists attempts to block spam by IP address by associating a large, rapidly changing list of DNS records with a single domain name. These DNS records use the IP addresses of compromised hosts that are part of a botnet and act as proxies to disguise the source. Since the IP addresses change rapidly, IP-based access control countermeasures are ineffective.[41]

Botnets are not used only for spam; they are also used to install malware and commit distributed denial of service attacks. As such, there are many efforts to combat botnets and the public and private sectors have worked together on this problem. To date, law enforcement officials have shut down many different botnets, including some that were responsible for sending a substantial amount of the world's spam. Shutting down botnets is complicated and resource-intensive, and each botnet presents different challenges.

Consider the case of "Grum." The Grum botnet has been in operation since February 2008. As of July 2012, it was estimated to have infected over half a million computers and to have sent 17 percent of the world's spam from 120,000 different IP addresses.[42] At that time, private sector security firms worked with law enforcement officials to understand how the botnet worked and to identify the IP addresses of the command and control servers. They found that the botnet operators were using servers located in the Netherlands, Panama, and Russia. Criminals frequently try to base their servers in countries where law enforcement is less responsive. After the servers were identified, Dutch officials took down the servers in the Netherlands, but the Internet service providers (ISPs) in Russia and Panama ignored requests from the security community to shut down the other servers. A few days later the Panamanian ISP shut down the botnet's server in Panama in response to international pressure. During this time, the botnet operators began redirecting the infected computers to new servers in Ukraine.[43] Shortly after being notified, the Ukraine ISP shut down access to these servers. The Russian ISP continued to ignore requests; however its upstream provider shut down routing to the IP addresses of the last of the botnet's command and control servers.[44] This should have been the end of the story for Grum. But a few days later, the Ukrainian ISP opened up access to the new Ukrainian servers for unknown reasons. After further complaints, the ISP agreed to shut down access to these servers permanently.[45] Overall, the takedown of the Grum botnet was easier than most because the botnet was not designed to be particularly robust. However, as botnets evolve they will continue to become more and more resistant to takedown attempts. As is the case in many cybercrimes, authorities have not been able to identify the individuals involved in running the Grum botnet and no charges have been filed. Law enforcement officials often have difficulty with attribution because individuals hide their tracks by using aliases and transferring funds anonymously online. When spam is used to sell physical products, these are often shipped from India (pharmaceuticals) or China (replica

watches).[46] Spammers may also use a technique called "drop shipping" where orders are passed on to a third party for fulfillment.

Unfortunately, attempts to take down botnets may be successful in the short-term, but not in the long-term. Even when the command and control servers are discovered and taken down by law enforcement, botnet operators may be able to recover control of many of their infected hosts. For example, the "Virut" botnet had a footprint of approximately 300,000 machines and has been active since 2006. The botnet has been used for a variety of criminal activities, including launching distributed denial of service attacks and sending spam. In 2013, Polish investigators seized twenty-three domains that were being used to operate the botnet. Unfortunately, the Virut botnet included a failsafe so that if the hardcoded domain names for the command and control servers were ever taken down, the infected machines would redirect themselves to a set of randomly generated domains that could be computed only by the botnet operator.[47] In addition, to prevent law enforcement officials from seizing control of the botnet, botnet operators have begun to use more advanced cryptography to authenticate connections between infected machines and command and control servers. Taking down the command and control server does not eliminate the threat since the computers that make up the botnet are still infected with malware. Once the Polish authorities had seized the domains used by Virut, an incident response team began working to alert users of their infected machines and help them clean them.[48] Removing malware from a large number of computers can require substantial resources. As with Grum, law enforcement officials have not yet identified the individuals responsible for operating the botnet or for creating the malware.

In the past, spammers would rent servers directly and use them for spamming until they got shut off by the hosting company once the illegal use was detected or the IP addresses used by spammers got blacklisted. Once this happened, they would move on to another hosting company or open a new account under another name. Since they could do this remotely and anonymously, they did not expose themselves to much risk of prosecution. However, to further protect their identities and operate more efficiently, spammers often use intermediaries offering "bulletproof hosting." Unlike a legitimate hosting provider, bulletproof hosts tolerate illegal uses.[49] Bulletproof hosts offer web hosting and domain registration services to spammers and others engaged in illegal activity. Businesses that do this openly in law-abiding countries have been shut down. Two examples are the U.S.-based hosting providers McColo and 3FN. In the case of McColo, the upstream ISPs shut it down in 2008 after a high-profile news story in *The Washington Post* identified it as a prominent source of spam, malware, and child pornography. However, law enforcement officials have not pursued charges against the company owners.[50] Although hosting companies generally are not liable for illegal activity on their networks, those that abet illegal activity can be prosecuted under U.S. law. Proving that a company is facilitating illegal activity is not always easy, but it has been done. In June 2009, the FTC received a court order to temporarily shut down the hosting provider 3FN; a year later a judge ruled that the ISP be permanently shut down, its assets seized and sold, and the $1 million in revenue from its operation turned over to the government.[51] However, no individuals have faced criminal prosecution in this case either.[52]

Bulletproof hosting service providers typically are virtual middlemen on the black market who resell online services from legitimate ISPs to cybercriminals. Some, such as TowPow, even advertise themselves to cybercriminals as "Made by Spammers, for Spammers."[53] The bulletproof hosting service provider will monitor the IP addresses of the servers they are reselling and relocate their clients' data to different computers and networks once security firms flag the IP addresses as suspicious or the ISP shuts them down. As with others engaged in illegal online activities, bulletproof hosting operators use the anonymity of the Internet and anonymous digital cash transactions to disguise their identity as much as possible and avoid prosecution.[54] The use of bulletproof hosting also makes it more difficult to catch the criminals at the top, since law enforcement officials are more likely to track down low-level bulletproof hosting operators than the individuals operating botnets and writing malware. This means that, as with other criminal syndicates, law enforcement efforts may end up going after the middlemen who are easily replaced rather than the masterminds at the top.

Successfully prosecuting spam cases requires a significant level of resources, in particular to identify and locate the individuals responsible for spam, coordinate law enforcement cooperation across many different jurisdictions, and build the technical evidence needed for a successful prosecution. For example, investigators in the Computer Crimes Section at the Virginia Attorney General's office spent the better part of a year bringing a case against Jeremy Jaynes.[55] This does not include additional resources spent by others, such as ISPs, who had to cooperate with the investigation, or the time spent responding to Jayne's (ultimately successful) appeals. However, even with these challenges, law enforcement officials have successfully gone after some of those in the cybercrime value chain, including individuals who write malware, operate botnets, and offer bulletproof hosting. For example, in 2005, an eighteen--year-old Muscovite named Nikita Kuzman wrote "Gozi," malware that has infected over a million computers worldwide, surreptitiously stealing banking passwords and other information. It originally targeted European banks, but then began targeting U.S. banks in 2010, prompting U.S. law enforcement to get involved. Later that year, U.S. investigators arrested Kuzmin on a trip to the United States and he pled guilty in May 2011. Latvian police arrested his accomplice, who allegedly created specific code for each targeted bank, about a year and a half later, and Romanian officials arrested the man who was allegedly providing them bulletproof hosting.[56] In January 2013, the U.S. Department of Justice unsealed indictments against all three individuals and announced that it had initiated extradition proceeding for the two men in Latvia and Romania. The individuals face a maximum penalty for the charges of between sixty to ninety-five years.[57]

Overall, the underground Internet economy displays a surprising amount of entrepreneurship and innovation. Pay-per-install schemes entice "entrepreneurial malware distributors" to come up with innovative ways to infect PCs since they get paid for every successful installation. Middlemen set up shop to streamline criminal activities, such as renting botnets, buying email account credentials, providing bulletproof hosting, and offering CAPTCHA solvers. (A CAPTCHA is a short puzzle presented on a web page that should require a human to solve. Spammers use automated CAPTCHA solvers to circumvent this countermeasure employed by websites to prevent abuses.) Anonymous

individuals offer to sell stolen or harvested email lists to spammers. Payment processors anonymously transfer funds between illicit businesses. Programmers release updates to malware toolkits that exploit the latest security vulnerabilities. As with other areas of the Internet economy, the criminal side is driven by competition, profits, specialization, and complex business relationships.

WHAT MORE CAN GOVERNMENT DO?

Sending spam is cheap, profitable, and low-risk. As long as the benefits of sending spam outweigh the costs, unscrupulous individuals will always be motivated to send spam. Those interested in reducing spam have two options: raise the costs or reduce the benefits of sending spam. For example, on the technology side, anti-spam software decreases the expected benefits for spammers by blocking more spam from consumers; on the policy side, higher penalties and levels of enforcement increase the expected costs for spammers. Since spam imposes a substantial financial cost on businesses and consumers, policymakers should take more aggressive action both domestically and internationally.

Since spam imposes a substantial financial cost on businesses and consumers, policymakers should take more aggressive action both domestically and internationally.

Develop and deploy comprehensive cybersecurity countermeasures

Policymakers should recognize that the volume of spam is indicative of widespread security vulnerabilities in computer systems and networks, and that reducing spam necessarily involves addressing these security weaknesses. Developing stronger cybersecurity countermeasure can help deter spam by raising costs for spammers and reducing their potential earnings. Efforts to combat spam operations may have a displacement effect on other cybercrime, such as motivating botnet operators to focus on other profitable illegal activity. Following various efforts in 2010 to reduce spam, the total volume of spam decreased substantially, but the number of distributed denial of service attacks during this period increased. This suggests that spam should be addressed as part of a holistic approach to cybersecurity. One important approach is for the United States and other countries to continue to invest heavily in cybersecurity research and development.[58] The U.S. Department of Homeland Security Science and Technology Directorate identified combatting malware and botnets as one of the eleven "hard problems" in cybersecurity that the U.S. government should focus on funding, in part because of the use of botnets to send spam.[59] Researchers need to stay ahead of the criminals to effectively combat cybercrime.

In addition, it is not enough to simply develop effective security technology; it must also be deployed. To that end, policymakers should work with industry to increase the use of effective computer and network security products, services and best practices. For example, the Communications Security, Reliability and Interoperability Council, an advisory committee to the Federal Communications Commission, established a working group to investigate botnet remediation in broadband networks and produced a voluntary U.S. Anti-Bot Code of Conduct for ISPs.[60] Other similar codes of conduct may be useful as well. For example, the Department of Justice and the Federal Trade Commission could develop best practices for e-commerce sites that use affiliate marketing programs since these programs may be abused by spammers. Best practices such as these should be promoted not only domestically, but internationally.

As noted earlier, individuals have different experiences with spam, in part because some organizations do not use effective spam filters or domain-based message authentication.[61] While poor security has a direct impact on organizations, it imposes an even greater negative externality on the rest of society. Smaller organizations, in particular, are likely to lack the technical expertise necessary to differentiate between different computer security products, including anti-spam technology. In the United States, the Small Business Administration (SBA) produces a number of guides to help business owners. The SBA and similar agencies in other countries could also produce a series of guides for business owners on how better to protect against security threats, including spam, and evaluate different product offerings. In addition, organizations may not be aware of the productivity costs implicit in their choice of anti-spam technology. Governments should lead by example and include these productivity losses from spam in their own evaluations and procurement of enterprise email products and anti-spam technology.

Enhance cybercrime law enforcement efforts and capabilities

Governments should increase the resources available to take law enforcement actions against cybercriminals, especially those knowingly facilitating spam and other related Internet crime. Investigating and prosecuting cybercrime is frequently difficult, resource-intensive, and involves multiple jurisdictions and agencies both domestically and internationally. While there have been a number of successful law enforcement efforts to date, given the large negative externalities from spam and the magnitude of the problem today, it is likely that additional government effort would be beneficial. Legislative bodies in the United States, Europe and other countries should expand funding available to law enforcement agencies to facilitate information sharing, coordination, training, and outreach to combat spam and related crime. Towards that end, the U.S. Congress should fully fund the U.S. Department of Justice (DOJ) FY 2014 budget request which includes expanding the cybersecurity criminal division.[62]

As part of the effort to increase resources dedicated to fighting spam and other forms of cybercrime, the private sector should be allowed to play a greater role. Law enforcement officials already partner with private-sector companies to combat cybercrime since it is these companies' systems that are often being targeted or used to carry out attacks and they often have better insight into many of the threats.[63] In addition, the private sector has some of the leading technical experts who are able to uncover the technical functionality of threats such as malware and botnets. However, more could be done.

Currently, the private sector is limited in what it can do depending on the circumstances. The private sector has three primary options. First, it can simply assist law enforcement with their operations or bring cases to their attention. Second, it can take extrajudicial actions to shut down potentially illegal operations by filing complaints with the host network or even by launching counter-cyber-attacks against suspected criminals. The risk of this type of activity is that the companies in the private sector would be liable for damages as a result of their actions. Third, it can use civil legal proceedings against suspected criminals. In one notable case, the cybercrime division at Microsoft worked with the FBI and other law enforcement officials around the world to obtain a court order to seize hundreds of domains and servers being used as part of a botnet.[64] To enable industry

to play a greater role, law enforcement officials should consider developing a "cyber-deputy" program both to set guidelines for this cooperation and to provide liability protection for private-sector efforts.[65] This will ensure that such efforts are encouraged and utilized, while not disrupting or impeding ongoing criminal investigations.

Different laws are used to prosecute different types of spammers. While anti-spam laws are sometimes used, and countries without anti-spam laws should adopt them, it often makes sense to prosecute spammers or their accomplices for other violations, including intellectual property crimes, computer fraud, wire fraud, money laundering, or other crimes in connection with their involvement in organized crime syndicates.[66] Strong laws are necessary to deter and prosecute cybercrime. In the United States, Congress should update the Computer Fraud and Abuse Act (CFAA) to ensure that law enforcement officials can prosecute those engaged in cybercrime and that the law served as a deterrent to cybercrime. The maximum penalties for certain types of unauthorized access to computer systems remain low (e.g. five years in prison) even for substantive crimes such as stealing a database of 100,000 credit card numbers.[67] Yet, after the suicide of Internet activist Aaron Swartz, some organizations have begun pushing for the elimination of criminal penalties under the CFAA for violations of a computer system's terms of service.[68] Updates to the CFAA should make it clear that minor violations, such as using a fake name on a social network or a fake weight on an online dating profile in violation of a website's terms of service are not felonies.[69] However, more serious violations, especially those designed to obtain high-value information or sensitive personal information, or those executed in the process of committing other crimes, should be treated as the serious criminal acts they are.[70] Any update to the CFAA should establish limits on the conditions under which the law is applied, and prosecutors should exercise discretion appropriately, but the law should be strengthened to prosecute those engaged in or facilitating cybercrime.

Promote international efforts to combat spam

While there are some important actions countries can take on their own, ultimately reducing the problem of spam will require international cooperation. The global nature of the Internet allows spammers to operate from countries where sending spam is not illegal or where laws are loosely enforced. As one pair of security researchers noted, "A spammer may be based in Latvia, work for a merchant in Moscow, send spam to the United States from a botnet with zombie computers all over the world, and have the final goods shipped from India."[71]

Multiple international bodies have endorsed efforts to reduce spam and promote cybersecurity. For example, the 2003 Declaration of Principles of the World Summit on the Information Society (WSIS) notes, "Spam is a significant and growing problem for users, networks and the Internet as a whole. Spam and cybersecurity should be dealt with at appropriate national and international levels."[72] More recent efforts to promote international cooperation on spam have been rejected, most notably at the 2012 International Telecommunication Union (ITU) World Conference on International Telecommunication (WCIT-12).[73] There, many countries, including the United States, did not sign the revised international telecommunication regulations (ITRs) because of concerns about proposals on spam, cybersecurity and internet governance.[74] Some delegates

from these countries were concerned that countries wishing to impose surveillance or censorship on its citizens would use the spam proposal as justification for this action.[75] While it is impossible to say how countries may try to distort their interpretation of a treaty, the language of the proposal on spam was clearly about developing technical measures, industry partnerships, educational efforts, and international cooperation to reduce spam.[76] While the U.S. may have had legitimate reasons for not signing the ITRs, the spam resolution should not have been one of them.[77] Because spam is an international problem with legitimate government interests, countries need a forum to discuss solutions. If U.S. policymakers are opposed to working within the ITU to resolve the issue of spam, then they should propose an alternative forum where government and industry stakeholders can address spam and related issues, including through existing organizations working on related problems such as Interpol, FIRST (the global organization for regional Computer Emergency Response Teams, or CERTs), M3AAWG, and the Internet Society, to name a few.

If U.S. policymakers are opposed to working within the ITU to resolve the issue of spam, then they should propose an alternative forum where government and industry stakeholders can address spam and related issues.

Because cybercrime is global, in addition to participating in international bodies, U.S. law enforcement agencies and private-sector businesses must continue to work directly with their counterparts in other countries. As such, Congress should avoid legislation that prohibits engaging in international partnerships with other countries. Rep. DeSantis (R-FL) proposed an amendment to 2014 defense policy bill that would prohibit the United States from using funds to collaborate on cybersecurity activities with China, including participating in working groups.[78] Previous engagement with China to reduce spam has been positive and beneficial and such activities should be encouraged.[79]

Finally, because of the international nature of spam, the United States and its allies should work to ensure that efforts to improve cybersecurity, including reducing spam, are included in future trade agreements, such as the Transatlantic Trade and Investment Partnership (TTIP). Nations that seek to participate in agreements like the TTIP should commit to enacting robust cybersecurity legislation and enforcing it.

Implement a "name and shame" program

Some individuals and organizations intentionally help cybercriminals; others offer inadvertent aid through lax policies. While the former should be prosecuted, a more effective approach for the latter would be to implement a "name and shame" program to highlight the worst offenders. For example, the DOJ could produce an annual list of countries that do not cooperate with cybercrime law enforcement efforts. Similarly, the DOJ could work with industry to compile a list of ISPs, domain registrars, e-commerce affiliate programs, and others that do not respond to complaints about abuses. This would be similar to the Section 301 report produced by the Office of the United States Trade Representative (USTR) that identifies trade barriers in other countries that result from inadequate intellectual property laws and enforcement. One particularly effective strategy might be to identify the banks that process credit cards for spam merchants. Previous research has found that there are only a few foreign banks that process these payments. If U.S. law enforcement officials produced a list of these foreign banks, they could ask domestic banks to cease transacting with any foreign banks on the list. Other countries

should take similar steps to identify ISPs, domain registrars, banks and other stakeholders within their own borders who are aiding cybercriminals through weak policies.

Finally, one of the challenges in law enforcement for cyber-crime is identifying the individuals responsible for operating botnets and writing malicious code. These individuals are able to use the anonymity of the Internet to escape prosecution. Law enforcement officials should expand the use of monetary rewards for information that leads to the arrest or conviction of individuals engaged in cybercrime. For example, the Department of Justice could operate a "Ten Most Wanted List" for botnet operators. Not only might this help lead to some successful prosecutions, it would also create pressure on spammers and other criminals to reduce their illicit activities so as not to draw attention to themselves. Bounty programs have been a useful tool for fighting other types of organized crime.[80]

CONCLUSION

In short, spam is a problem without an easy solution, but there is more that government can and should do. In particular, spam must be addressed as part of a comprehensive effort to improve cybersecurity.

ENDNOTES

1. Brad Templeton, "Reactions to the DEC spam of 1978," n.d., http://www.templetons.com/brad/spamreact.html.
2. Symantec reports a similar peak in July 2010, but a lower total volume of approximately 230 billion spam messages. See Laura Atkins, "Spam Volumes In 2010" CircleID, January 3, 2011, http://www.circleid.com/posts/20110103_spam_volumes_in_2010/ and Martin Lee, "Why My Email Went," Symantec, June 29, 2011, http://www.symantec.com/connect/blogs/why-my-email-went.
3. Cisco, "Spam Overview" n.d., http://www.senderbase.org/static/spam.
4. Ibid.
5. The exact percent varies from month to month. Historically, botnets have sent between 60 to 90 percent of spam. See James Delahunty, "Global spam volume drops one-third following Rustock takedown," Afterdawn, March 31, 2011, http://www.afterdawn.com/news/article.cfm/2011/03/31/global_spam_volume_drops_one-third_following_rustock_takedown.
6. Trend Micro, "TrendsLabs 2012 Annual Security Roundup: Evolved Threats in a 'Post-PC' World," 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-evolved-threats-in-a-post-pc-world.pdf.
7. Sophos, "Security Threat Report 2013," 2013, http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx.
8. Brian Krebs, "Spam Volumes: Past & Present, Global & Local," Krebs on Security, January 15, 2013, http://krebsonsecurity.com/2013/01/spam-volumes-past-present-global-local/.
9. Karl Rauscher and Yonglin Zhou, "Fighting Spam to Build Trust," EastWest Institute, May 27, 2011, http://www.ewi.info/fighting-spam-build-trust.
10. Justin M. Rao and David H. Reiley, "The Economics of Spam," *Journal of Economic Perspectives* (2012), 26(3): 87-110. http://www.aeaweb.org/articles.php?doi=10.1257/jep.26.3.87.
11. Rao and Reiley, "The Economics of Spam."
12. "March 2012 VBSPAM Comparative Review," Virus Bulletin, March 2012, http://www.virusbtn.com/pdf/magazine/2012/201203-vbspam-comparative.pdf
13. Rick Broida, "Gmail tip: Don't forget to check your spam filter," PCWorld, May 31, 2013, http://www.pcworld.com/article/2040415/gmail-tip-dont-forget-to-check-your-spam-filter.html.
14. Gallup/USA Today Poll, Oct, 2011. Retrieved Jun-17-2013 from the iPOLL Databank, The Roper Center for Public Opinion Research, University of Connecticut. http://www.ropercenter.uconn.edu/data_access/ipoll/ipoll.html and Gallup/USA Today Poll, Jan, 2011. Retrieved Jun-17-2013 from the iPOLL Databank, The Roper Center for Public Opinion Research, University of Connecticut. http://www.ropercenter.uconn.edu/data_access/ipoll/ipoll.html.
15. Deborah Fallows, "Spam 2007: Data Memo," Pew Internet and American Life Project, May 23, 2007, http://www.pewinternet.org/Reports/2007/Spam-2007/Data-Memo.aspx.
16. Steven Gray, "Straight to the Spam Folder: Astonishing E-Mail Messages You'll Never Open," PCWorld, 2009, http://www.pcworld.com/article/171349/spam_folder_favorites.html.
17. Ferris Research, "The Global Economic Impact of Spam, 2005," Report #409, February 2005.
18. Jenny S. Durkan, "Investigating And Prosecuting 21st Century Cyber Threats," Statement before the Committee On Judiciary, Subcommittee On Crime, Terrorism, Homeland Security, and Investigations, United States House Of Representatives, March 13, 2013, http://judiciary.house.gov/hearings/113th/03132013_2/Durkan%2003132013.pdf.
19. "eMail Industry Statistics," The Museum of Email and Digital Communications, n.d., http://email-museum.com/reports/industry-statistics/.
20. Rao and Reiley, "The Economics of Spam."
21. Ibid.
22. For an example of a pump and dump scam, see "Organizer Of International Securities Fraud Ring Perpetrated Through Botnets And Stock Manipulation Convicted," U.S. Attorney's Office, District of New Jersey, November 30, 2012, http://www.justice.gov/usao/nj/Press/files/Rad,%20Christopher%20Verdict%20PR.html.

23. Brian Krebs, "Polish Takedown Targets 'Virut' Botnet," Krebs on Security, January 18, 2013, http://krebsonsecurity.com/2013/01/polish-takedown-targets-virut-botnet/.
24. Graham Cluley, "Father's Day spam floods in, pointing to gambling websites," Naked Security, June 14, 2012, http://nakedsecurity.sophos.com/2012/06/14/fathers-day-spam-floods-in-pointing-to-gambling-websites/.
25. "Security Threat Report 2013," Sophos, 2013, http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx.
26. U.S. Federal Trade Commission, "FTC Cracks Down on Senders of Spam Text Messages Promoting 'Free' Gift Cards," March 7, 2013, http://www.ftc.gov/opa/2013/03/textmessages.shtm.
27. Jan Lauren Boyles, "Mobile Phone Problems," Pew Internet & American Life Project, August 2, 2012, http://pewinternet.org/Reports/2012/Mobile-phone-problems.aspx.
28. Rao and Reiley, "The Economics of Spam."
29. "2013 Threats Predictions," McAfee Labs, 2013, http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf.
30. Boyles, "Mobile Phone Problems."
31. See Articles I-9, I-10 and I-11 in "Draft African Union Convention on the Confidence and Security in Cyberspace," Economic Commission for Africa and African Union Commission, January 1, 2013, http://pages.au.int/sites/default/files/AU%20Cybersecurity%20Convention%20ENGLISH_0.pdf.
32. U.S. Federal Trade Commission, "The U.S. SAFE WEB Act: The First Three Years," December 2009, http://www.ftc.gov/os/2009/12/P035303safewebact2009.pdf.
33. See "State Laws: Summary," SpamLaws.com, n.d., http://www.spamlaws.com/state/summary.shtml (accessed June 1, 2013) and "Summary of State Laws," Direct Marketing Association, May 9, 2003, http://www.the-dma.org/antispam/statespamlaws.shtml.
34. "Deterring Malicious Spammers and Cybercriminals" panel discussion at FTC Spam Summit: The Next Generation of Threats and Solutions, July 11, 2007, http://www.ftc.gov/bcp/workshops/spamsummit/presentations/Law-Enf.pdf.
35. Austin Modine, "Virginia de-convicts AOL junk mailer Jeremy Jaynes," The Register, September 13, 2008, http://www.theregister.co.uk/2008/09/13/virginia_overturns_antispam_conviction/.
36. "About Spamhaus," Spamhaus, n.d. http://www.spamhaus.org/organization/ (accessed June 1, 2013).
37. "The Top 10 Worst," Spamhaus, June 1, 2013, http://www.spamhaus.org/statistics/networks/.
38. Gilou Tenebro, "W32.Waledac Threat Analysis," Symantec, 2009, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/W32_Waledac.pdf.
39. Eduard Kovacs, "Waledac Malware Could Send 3.6 Billion Spam Emails per Day from Infected PCs," Softpedia, January 15, 2013, http://news.softpedia.com/news/Waledac-Malware-Could-Send-3-6-Billion-Spam-Emails-Per-Day-From-Infected-PC-321404.shtml.
40. Nart Villeneuve, Jessa dela Torre, and David Sancho, "Asprox Reborn," TrendMicro, 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-asprox-reborn.pdf.
41. This "snowshoe" method of sending out lots of messages from legitimate IP addresses makes it difficult to block spammers. "2013 Threats Predictions," McAfee Labs, 2013, http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf.
42. "Security Threat Report 2013," Sophos, 2013, http://www.sophos.com/en-us/security-newsr-trends/reports/security-threat-report.aspx.
43. Atif Mushtaq, "Killing the Beast – Part 5," FireEye Blog, July 9, 2012, http://www.fireeye.com/blog/technical/botnet-activities-research/2012/07/killing-the-beast-part-5.html, Atif Mushtaq, "Grum CnCs—Just a few more to go," FireEye Blog, July 17, 2012, http://www.fireeye.com/blog/technical/botnet-activities-research/2012/07/grum-cncs-just-a-few-more-to-go.html, and Atif Mushtaq, "Grum, World's Third-Largest Botnet, Knocked Down," FireEye Blog, July 18, 2012, http://www.fireeye.com/blog/technical/botnet-activities-research/2012/07/grum-botnet-no-longer-safe-havens.html.
44. Ibid.
45. Atif Mushtaq, "Grum—The Money Factor," FireEye Blog, July 23, 2012, http://www.fireeye.com/blog/technical/botnet-activities-research/2012/07/grum-the-money-factor.html.

46. Rao and Reiley, "The Economics of Spam."
47. Nicolas Falliere, "W32.Virut: Using Cryptography to Prevent Domain Hijacking," Symantec, August 24, 2011, http://www.symantec.com/connect/blogs/w32virut-using-cryptography-prevent-domain-hijacking.
48. Brian Krebs, "Polish Takedown Targets 'Virut' Botnet," Krebs on Security, January 18, 2013, http://krebsonsecurity.com/2013/01/polish-takedown-targets-virut-botnet/.
49. Robert McMillan, "In China, $700 Puts a Spammer in Business," CIO, May 8, 2009, http://www.cio.com/article/492113/In_China_700_Puts_a_Spammer_in_Business.
50. This might be due, in part, to the fact that its alleged founder was a nineteen-year-old Russian who died in a car accident that year. Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, (O'Reilly Media, December 12, 2011), p. 127.
51. "FTC v. Pricewert," Civil Action No. 09-CV-2407, Federal Trade Commission, June 3, 2009, http://www.ftc.gov/os/caselist/0923148/.
52. Brian Krebs, "The Fallout from the 3FN Takedown," Security Fix blog on *Washington Post*, June 10, 2009, http://voices.washingtonpost.com/securityfix/2009/06/the_fallout_from_the_3fn_taked.html.
53. Brian Krebs, "Inside the Gozi Bulletproof Hosting Facility," Krebs on Security, January 25, 2013, http://krebsonsecurity.com/2013/01/inside-the-gozi-bulletproof-hosting-facility/.
54. Nate Anderson, "How the feds put a bullet in a "bulletproof" Web host," Ars Technica, January 23, 2013, http://arstechnica.com/security/2013/01/how-the-feds-put-a-bullet-in-a-bulletproof-web-host/.
55. "Deterring Malicious Spammers and Cybercriminals" panel discussion at FTC Spam Summit.
56. Krebs, "Inside the Gozi Bulletproof Hosting Facility."
57. "Three Alleged International Cyber Criminals Responsible for Creating and Distributing Virus That Infected Over One Million Computers and Caused Tens of Millions of Dollars in Losses Charged in Manhattan Federal Court," Federal Bureau of Investigation, New York Field Office, January 23, 2013, http://www.fbi.gov/newyork/press-releases/2013/three-alleged-international-cyber-criminals-responsible-for-creating-and-distributing-virus-that-infected-over-one-million-computers-and-caused-tens-of-millions-of-dollars-in-losses-charged-in-manhattan-federal-court.
58. The President's budget proposed nearly $500 million in R&D in cybersecurity for 2014. See "The Budget," Office of Management and Budget, 2013, http://www.whitehouse.gov/omb/budget/Overview.
59. "A Roadmap for Cybersecurity Research," Department of Homeland Security, November 2009, http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf.
60. "Final Report: U.S. Anti-Bot Code of Conduct (ABC) for Internet Service Providers (ISPs)," Communications Security, Reliability and Interoperability Council, March 2013, http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.
61. "2013 Honor Roll Report," Online Trust Alliance, 2013, https://otalliance.org/resources/2013honorRoll/2013Report.html.
62. "FY 2014 Budget Request: Cyber Security," U.S. Department of Justice, 2013, http://www.justice.gov/jmd/2014factsheets/cyber-security.pdf.
63. John Ribeiro, "Microsoft, US feds disrupt Citadel botnet network," ComputerWorld, June 5, 2013, http://www.computerworld.com/s/article/9239861/Microsoft_US_feds_disrupt_Citadel_botnet_network.
64. Brian Krebs, "Microsoft Takes Down Dozens of Zeus, SpyEye Botnets," Krebs on Security, March 26, 2012, http://krebsonsecurity.com/2012/03/microsoft-takes-down-dozens-of-zeus-spyeye-botnets/, Brian Krebs, "Microsoft Responds to Critics Over Botnet Bruhaha," Krebs on Security, April 16, 2012, http://krebsonsecurity.com/2012/04/microsoft-responds-to-critics-over-botnet-bruhaha/ and Antone Gonsalves, "Microsoft criticized for botnet takedown tactics," CSO, June 13, 2013, http://www.csoonline.com/article/734812/microsoft-criticized-for-botnet-takedown-tactics.
65. As a McAfee reports notes, "There is a massive liability issue associated with the unauthorized remote operation of systems, even with the best of intentions." "2013 Threats Predictions," McAfee Labs, 2013, http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf.
66. For a list of spam laws worldwide, see "Anti-Spam Laws and Authorities Worldwide," International Telecommunication Union, n.d. http://www.itu.int/osg/spu/spam/law.html.
67. Jenny S. Durkan, "Investigating And Prosecuting 21st Century Cyber Threats," Statement before the Committee On Judiciary, Subcommittee On Crime, Terrorism, Homeland Security, and Investigations,

United States House Of Representatives, March 13, 2013, http://judiciary.house.gov/hearings/113th/03132013_2/Durkan%2003132013.pdf.
68. See discussion draft Zoe Lofgren, "Aaron's Law," 113th Congress, January 30, 2013, http://www.lofgren.house.gov/images/stories/pdf/aarons%20law%20revised%20draft%20013013.pdf.
69. Orin S. Kerr, "Cyber Security: Protecting America's New Frontier," Before the Subcommittee on the Crime, Terrorism, and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, November 15, 2011, http://www.volokh.com/wp-content/uploads/2011/11/Testimony-of-Orin-S-Kerr.pdf.
70. "Charging Documents: U.S. v. Nikita Kuzmin, U.S. v. Mihai Ionut Paunescu, and U.S. v. Deniss Calovskis," U.S. State Attorney's Office, Southern District of New York, January 23, 2013, http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusDocuments/Paunescu,%20Mihai%20Ionut%20Indictment.pdf.
71. Rao and Reiley, "The Economics of Spam."
72. "Building the Information Society: a global challenge in the new Millennium," World Summit on the Information Society, December 12, 2003, http://www.itu.int/wsis/docs/geneva/official/dop.html.
73. Richard Bennett, "The Gathering Storm: WCIT and the Global Regulation of the Internet," Information Technology and Innovation Foundation, November 2012, http://www2.itif.org/2012-gathering-storm-wcit-regulations.pdf.
74. Samantha Bookman, "U.S. refuses to sign WCIT-12 treaty; controversial document gives ITU more Internet control," FierceTelecom, December 13, 2012, http://www.fiercetelecom.com/story/us-refuses-sign-wcit-12-treaty-controversial-document-gives-itu-more-intern/2012-12-13.
75. Emma Llansó, "Making Sense of the WCIT: It's Complicated!" Center for Democracy and Technology, December 20, 2012, https://www.cdt.org/blogs/emma-llanso/2012making-sense-wcit-it%E2%80%99s-complicated and Larry Downes, "Requiem for Failed UN Telecom Treaty: No One Mourns the WCIT," Forbes, December 17, 2012, http://www.forbes.com/sites/larrydownes/2012/12/17/no-one-mourns-the-wcit/.
76. "Resolution 52 – Countering and combating spam," International Telecommunication Union, World Telecommunication Standardization Assembly, Dubai, November 20-29, 2012, http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2012-PDF-E.pdf
77. "Criticism of the 2012 ITRs Not Valid, Says Former Senior ITU Official," Intellectual Property Watch , June 11, 2013, http://www.ip-watch.org/2013/06/11/criticism-of-the-2012-itrs-not-valid-says-former-senior-itu-official/.
78. Ron DeSantis, "Amendment to the Rules Committee Print of H.R. 1960," June 10, 2013, http://amendments-rules.house.gov/amendments/ChinaCyberAmend611130943214321.pdf.
79. Rauscher and Zhou, "Fighting Spam to Build Trust."
80. "Statement by the President on Enhanced State Department Rewards Program," The White House, January 15, 2013, http://www.whitehouse.gov/the-press-office/2013/01/15/statement-president-enhanced-state-department-rewards-program.

ACKNOWLEDGEMENTS

The author wishes to thank the following individuals for providing input to this report: Rob Atkinson and Sue Wunder. Any errors or omissions are the author's alone.

ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with the Information Technology and Innovation Foundation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

FOR MORE INFORMATION VISIT WWW.ITIF.ORG.