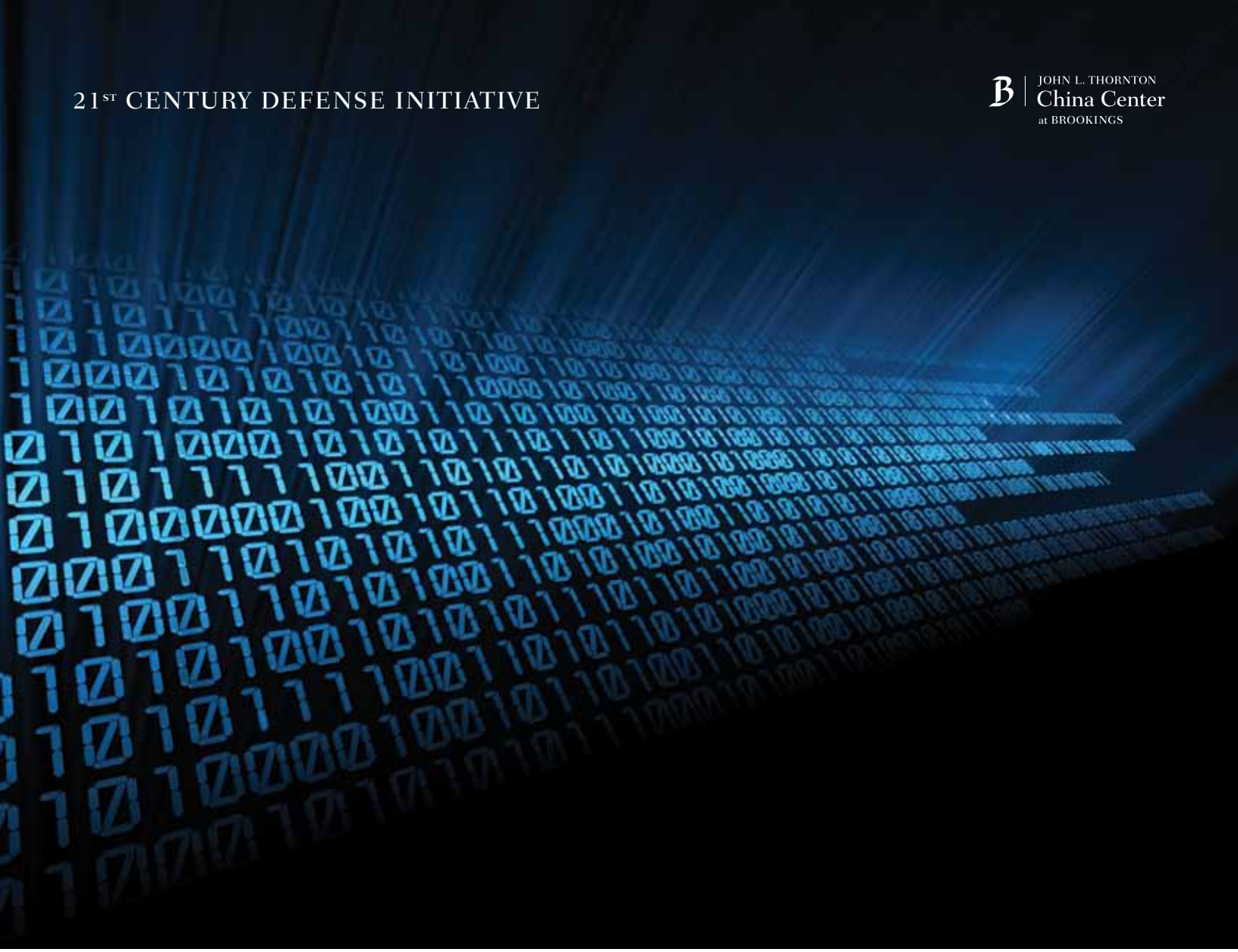
21ST CENTURY DEFENSE INITIATIVE

JOHN L. THORNTON China Center at BROOKINGS



CYBER SECURITY #1
JULY 2011

Foreign Policy at BROOKINGS

Pirates of the ISPs:
Tactics for Turning Online Crooks Into International Pariahs

Noah Shachtman

Pirates of the ISPs:
Tactics for Turning Online Crooks Into International Pariahs

Noah Shachtman

CYBERSECURITY #1
JULY 2011

21ST CENTURY DEFENSE INITIATIVE

JOHN L. THORNTON China Center at BROOKINGS

Acknowledgements

Every research paper is a group effort, no matter what it says on the byline. This project relied more on outside assistance than most. Brookings Senior Fellows Peter Singer and Ken Lieberthal were the ones who convinced me to explore the broad topic of cybersecurity. The panel they assembled gave me new insight with every meeting; my colleague Allan Friedman was an especially invaluable tutor and remarkably generous with his time. Heather Messera and Robert O'Brien provided important research and logistical support. My research assistant, Adam Rawnsley, was tireless in his exploration of the minutiae of everything from tort law to pirate havens.

My Wired.com colleagues—Ryan Singel, Kevin Poulsen, Kim Zetter and David Kravets—cover the cybersecurity beat better than anyone. This paper would have been impossible without them, and without Brian Krebs, master investigator of the online underworld.

Bill Woodcock, Rick Wesson, Jeff Cooper, Tyler Moore, Audrey Plonk, Jim Lewis, Dmitri Alperovitch, Paul Nicholas, Jessica Herrera-Flannigan, Jart Armin, Richard Bejtlich, Steve Schleien, Jonathan Zittrain and many, many others steered me away from my worst ideas and towards those few not-so-bad ones. For that, I am deeply in their debt.

Brookings recognizes that the value it provides to any supporter is in its absolute commitment to quality, independence and impact. Activities supported by its donors reflect this commitment and the analysis and recommendations are not determined by any donation.

Table of Contents

Executive Summary

At the beginning of the 19th century, piracy was an ongoing threat and an accepted military tactic. By the end of the century, it was taboo, occurring solely off the shores of failed states and minor powers. The practice of hijacking did not vanish entirely, of course; it is flourishing now on the world's computer networks, costing companies and consumers countless billions of dollars.

Cybercrime today seems like a nearly insoluble problem, much like piracy was centuries ago. There are steps, however, that can be taken to curb cybercrime's growth—and perhaps begin to marginalize the people behind it. Some of the methods used to sideline piracy provide a useful, if incomplete, template for how to get it done. Shutting down the markets for stolen treasure cut off the pirates' financial lifeblood; similar pushes could be made against the companies that support online criminals. Piracy was eventually brought to heel when nations took responsibility for what went on within its borders. Based on this precedent, cybercrime will only begin to be curbed when greater authority—and accountability—is exercised over the networks that form the sea on which these modern pirates sail.

In this new campaign, however, private companies, not governments, will have to play the central role, as Harvard's Tyler Moore and others have suggested. After all, the Internet is not a network of governments; it is mostly an amalgam of businesses that rely almost exclusively on handshake agreements to carry data from one side of the planet to another. The vast majority of the Internet's infrastructure is in the hands of these 5,000 or so Internet Service Providers (ISPs) and carrier networks, as is the ability to keep crooks off that infrastructure. If this relatively small group can be persuaded to move against online criminals, it will represent an enormous step towards turning these crooks into global pariahs.

The most productive thing ISPs can do to curb crime is put pressure on the companies that support and abet these underground enterprises. Currently, registration companies sell criminals their domain names, like "thief.com." Hosting firms provide the server space and Internet Protocol addresses needed to make malicious content online accessible. But without ISPs, no business, straight or crooked, gets online. A simple statistic underscores the ISPs' role as a critical intermediary: just 10 ISPs account for around 30 percent of all the spam-spewing machines on the planet.

ISPs are well aware of which hosting companies, for example, are the most friendly to criminals; lists of these firms are published constantly. But,

currently, ISPs have little motivation to cut these criminal havens off from the rest of the Internet. There is no penalty for allowing illicit traffic to transit over their networks. If anything, there is a strong incentive for maintaining business-as-usual: the hosting company that caters to crooks also has legitimate customers, and both pay for Internet access. So ISPs often turn a blind eye, even though the worst criminal havens are well-known.

That is where government could help. It could introduce new mechanisms to hold hosting companies liable for the damage done by their criminal clientele. It could allow ISPs to be held liable for their criminal hosts. It could encourage and regulate ISPs to share more information on the threats they find.

Government could also encourage more private businesses to come clean when they are victimized. Today, just three in ten organizations surveyed by the security firm McAfee report all of their data breaches. That not only obscures the true scope of cybercrime; it prevents criminals and criminal trends from being caught earlier. Government can alter that equation by expanding the requirements to report data breaches. It could require its contractors to purchase network security insurance, forcing companies to take these breaches more seriously. And it can pour new resources into and craft new strategies for disrupting criminals' support networks.

These steps will serve as important signals that America will no longer tolerate thieves and con artists operating on its networks. After all, 20 of the 50 most crime-friendly hosts in the world are American, according to the security researchers at HostExploit.

As the United States gets serious in curbing these criminals, it can ask more from—and work more closely with—other countries. China, for instance, sees itself as the world's biggest victim of cybercrime, even as it remains a hotbed for illicit activity. Not coincidentally, China is also only partially connected to the global community of ISPs. Dialogues to bring the Chinese closer into the fold will not only make it easier to marginalize cybercriminals; it will build momentum for broader negotiations on all sorts of Internet security issues.

Introduction

On May 22, 2009, nine pirates armed with rocket-propelled grenades began to chase the cargo ship *Maersk Virginia* as it steamed through the Gulf of Aden. The container vessel sped up to 21 knots, took evasive maneuvers, and let out a distress signal.[1] Among the first to respond to the hulking, 950 foot-long American hauler: An Iranian warship, volunteering its help. The pirates were run off before the offer could be accepted, but it wouldn't be the last time that putative enemies teamed up to stop the pirates off the Horn of Africa.[2] The Chinese Navy escorted Taiwanese vessels and Indian sailors freed their Pakistani counterparts after storming a pirate mothership through the same treacherous waters.

It is a sign of just how taboo piracy has become. Somali pirates have been captured by sailors from Sweden, South Korea and Russia, and charged in courts from New York to Mombassa to Kuala Lumpur. According to the United Nations Convention on the Law of the Sea, "every State" is authorized to "seize a pirate ship… arrest the persons and seize the property on board."[3] Piracy still continues, of course, but the sea-borne hijackers are forced to operate from the shores of the world's failed states, and are pursued by every major power on the planet. Not even terrorists are treated as such international pariahs.

It is a particularly striking turn of events given piracy's long history. For centuries, state-sanctioned pirates, or privateers, were accepted augmentations to traditional military forces. In the war against Spain, England's Queen Elizabeth I turned to privateers with a commission to plunder both hostile ships and enemy-held towns. American rebels in the Revolutionary War recruited 792 privateers who captured or destroyed 600 ships, and took 16,000 prisoners.[4] During the War of 1812, the American privateer fleet had more than 517 ships—compared to the U.S. Navy's 23.[5]

---

[1] Maersk Line Limited, "Maersk Virginia Approached By Pirates In The Gulf Of Aden," <http://www.maersklinelimited.com/News/pressreleases/2009/Maersk%20Virginia%20Approached%20by%20Pirates%20in%20the%20Gulf%20of%20Aden.pdf>.

[2] Sheila MacVicar, "Global Effort Clamps Down On Piracy," CBS News, May 29, 2009 <http://www.cbsnews.com/stories/2009/05/29/eveningnews/main5049947.shtml>.

[3] "Preamble to the United Nations Convention on the law of the Sea," <http://www.un.org/Depts/los/convention_agreements/texts/unclos/part7.htm>.

[4] Janice Thomson, Mercenaries, *Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe* (Princeton University Press, 1994) pgs. 25-26.

[5] American Merchant Marine and Privateers in War of 1812, accessed 5/9/2011, <http://www.usmm.org/warof1812.html>.

As the 19th century wore on, however, piracy and privateering not only fell out favor as a military tactic, it became taboo. London dismantled the markets for pirate booty. The Americans and the French launched attacks on the corsairs of the southern Mediterranean.

As Janice Thompson recounts in her seminal *Mercenaries, Pirates, and Sovereigns*, hijackers (and their state-approved counterparts) became marginalized as nations asserted greater control over their borders and established a monopoly on violence. In 1856, 42 nations agreed to the Declaration of Paris, which abolished privateering. The United States did not sign the document, but five years later, with America embroiled in its Civil War, President Abraham Lincoln refused to recruit the plunderers-for-hire—and blasted the Confederates as immoral for doing so themselves.[6] Two generations earlier, employing these hijackers had been a cornerstone of American naval strategy. By the 1860s, it was something civilized governments simply did not do.

The hijacking of money and goods has hardly stopped, but, aside from the Gulf of Aden, criminals have largely left the high seas. Today, they roam our computer networks. Last year, online thieves, extortionists, scammers and industrial spies cost businesses an estimated $43.5 billion in the United Kingdom alone, according to British government estimates.[7] Cybercrime is notoriously difficult to measure; assessments of the Internet's underground economy are guesses, at best. But if those British figures are even remotely accurate, firms worldwide could be facing the equivalent of hundreds of billions of dollars in losses every year.

As pervasive as cybercrime seems to be, however, there are steps that can be taken to curb its growth—and perhaps begin to sideline cybercrime, much as piracy was made unacceptable in a previous era. Some of the methods used to marginalize piracy provide a useful, if incomplete, template for how to stop cybercrime.

Shutting down the markets for stolen treasure cut off the pirates' financial lifeblood; similar pushes could be made against the companies that support the online criminals. Piracy was eventually brought to heel when nations assumed responsibility for what went on within their borders. Cybercrime will only begin to be curbed when greater authority and accountability are exercised over the networks that form the sea on which these modern pirates sail.

In this new push, however, it is private companies, not governments that will have to play the central role. After all, the Internet is not a network of governments. It is an array of businesses, mostly Internet Service Providers (ISPs) and network carriers that rely almost exclusively on handshake agreements to carry data from one side of the planet to another.[8] The vast majority of the Internet's infrastructure is in the hands of these 5,039 ISP and carrier networks as is the expertise to secure that infrastructure.

This also places Internet Service Providers in a unique position to help corral cybercrime, as Tyler Moore and Ross Anderson have observed.[9] Domain registrars can sell you a website name. So-called "hosting" companies can provide the server space and Internet Protocol addresses needed to make your content online accessible.

---

[6] William Morrison Robinson, Jr. *The Confederate Privateers*. (Yale University Press, New Haven, CT, 1928), pg. 14.
[7] Michel Holden, "Cyber crime costs UK $43.5 billion a year: study," Reuters, 2/17/2011, <http://www.reuters.com/article/2011/02/17/us-britain-security-cyber-idUSTRE71G35320110217>.
[8] Bill Woodcock, and Vijay Adhikari, "Survey of Characteristics of Internet Carrier Interconnection Agreements," Packet Clearing House, May, 2011.
[9] Tyler Moore and Ross Anderson, "Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research," in *The Oxford Handbook of the Digital Economy* (Oxford University Press, 2011).

But without ISPs, no business, straight or crooked, gets online. A simple statistic underscores the ISP's role as a critical intermediary. According to research conducted for the Organization for Economic Development and Cooperation, just 10 ISPs out of the 5,000+ worldwide account for around 30 percent of all the spam-spewing machines on the planet.[10]

Therefore, the first—and probably most important—step in creating a global taboo against online crooks is to persuade Internet Service Providers to turn against these scam artists and thieves and the companies that support them.

Currently, the ISPs do not have much motivation to take action. There is no penalty for allowing criminal traffic to transit over their networks. Nor is there much of a reward for throttling the hosting firms that give criminals the infrastructure to control their "botnets"—legions of hijacked computers. If anything, there is a strong incentive for maintaining business-as-usual practices: ISPs have traditionally shied away from policing the content on their networks. Besides, a hosting company that caters to crooks also has legitimate customers, and both pay for access to the Internet. As a result, ISPs often turn a blind eye, even though the worst criminal havens are well-known.

That is where government could help. It could introduce new mechanisms to hold hosting companies liable for the damages done by their criminal clientele. It could allow ISPs to be held liable for their criminal hosts. It could encourage ISPs to share more information on the criminal threats they find. Government could even provide public funds to help ISPs with the disinfection of their customers' machines, as Moore has suggested.[11]

Government could also encourage more private businesses to come clean when they are victimized. When online crooks strike, the overwhelming majority of companies stay quiet, fearing that such announcements could reveal a competitive weakness or invite more attacks. Just three in ten organizations surveyed by the security firm McAfee report all of their data breaches.[12] Hiding cyberattacks not only obscures the true scope of cybercrime, it prevents criminals and criminal trends from being caught earlier.

The flip side to the information issue is accountability. Currently, no one but the cybercriminal himself bears any responsibility for the spread of online crime. Software companies are not accountable when they ship out buggy code that criminals exploit. Registration firms are not responsible when they sell crooks the "badguy.com" domain from which they will do business. Hosting companies are not accountable when they give criminals the server space to house their scams. ISPs are not responsible when they connect those criminally-connected hosts to the rest of the Internet. Private companies shoulder no responsibility when their machines are infected and used to pull off crimes.[13] No wonder a "see no evil" attitude is so prevalent; fingers are always pointed in the other direction.

The federal government can alter that equation in one of several ways. It could expand today's requirements to report data breaches. It could require its contractors to purchase network security

---

[10] Michel van Eeten, Johannes M. Bauerb, et, al., "The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data," Organization for Economic Development and Cooperation, Directorate for Science, Technology and Industry, May, 2010, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.165.2211&rep=rep1&type=pdf>.

[11] Tyler Moore, "The Economics of Cybersecurity: Principles and Policy Options," *International Journal of Critical Infrastructure Protection,* Volume 3, Issues 3-4, 12/2010.

[12] McAfee and SAIC, "Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency," <http://www.mcafee.com/us/resources/reports/rp-underground-economies.pdf>.

[13] McAfee and SAIC.

insurance, forcing companies to take breaches more seriously. It could assign indirect liability for online thievery and scams, just like credit card companies are held indirectly liable for online gambling. And it could pour new resources into disrupting criminals' support networks.

All of these steps will serve as important signals that America will no longer tolerate thieves and con artists emanating from its networks. After all, the United States is, by some measures, the world's largest exporter of online crime. America has three times more spam havens than China,[14] and more than twenty times the number of fake banks, ersatz social networks and other so-called "phishing" sites.[15] America cannot reasonably demand that other countries get their houses in order until we show a willingness to do the same.

And as the United States gets more serious in curbing these criminals, it can ask more from—and work more closely with—other countries. Today, China and Russia are only partially connected to the global community of ISPs. Cooperation on cybercrime investigations is an ad hoc, largely disjointed affair, especially between Washington, Moscow and Beijing. That coordination has to improve, if there is to be a chance of seriously slowing online crime's rapid rise. There does not need to be an equivalent of 1856's global privateer ban to make an impact. As history shows, bi- and multilateral agreements in the 17th and 18th centuries affirmed the principles of open trade over the open seas. None of these documents explicitly abolished piracy; nor were they universally accepted, but they paved the way toward a global code of conduct that eventually turned pirates into international pariahs, pursued by all the world's major powers.

[14] Spamhaus, "The World's Worst Spam Producing Countries," accessed 5/8/2011, <http://www.spamhaus.org/>. statistics/countries.lasso

[15] OpenDNS, "2010 Report: Web Content Filtering and Phishing," <http://www.opendns.com/pdf/opendns-report-2010.pdf>.

What is Cybercrime?

Online crime has been notoriously tricky to define. Draw too wide a definition—as a recent Russia-U.S. bilateral group did—and the calculation of drug profits on Google Documents is suddenly labeled a cybercrime. After all, that is a use of "cyberspace for criminal purposes as defined by national or international law."[16] Make the definition too narrow—like one UN panel, which focused on "electronic operations that targets the security of computer systems"—and you exclude all the online crimes that rely on trickery instead of technical ability. For instance, one late 2010 con job that fooled executives at the Conde Nast publishing company into wiring $8 million to online scammers' accounts.[17]

Complicating matters further is the fact that, on the Internet, it is not always easy to tell a crook from a spy or a soldier. All three can use the same flaw in Internet Explorer to gain access to a computer. All three can use the same kind of software to scan for network holes. Whether the result of that intrusion is a crime, espionage or intelligence preparation of the battlefield is mostly up to the person who pulled off the break-in. It's largely a matter of intent.

For years, "hacking" was synonymous with felonious behavior and illicit network penetration. This is no longer the case. Yes, there are groups like Anonymous and Lulzsec that embrace the original hacker ethos—free information, technical prowess, and fun at the expense of the clueless—and yes, these groups can inflict harm on the organizations they target. But for the most part, the hacker community and the cybercrime underground have parted ways. Advanced technical skills are not necessarily required to pull off modern cybercrimes. Hardware and software makers that want to discover security flaws in their products—or discover new uses for these systems—often invite hackers to pull apart their wares. iRobot's Roomba autonomous vacuum cleaner and Microsoft's Kinect gaming controller are just two of many examples.[18] This does not mean that these hackers are criminals, and they should not be treated as such.

---

[16] Karl Frederick Rauscher and Valery Yaschenko, "Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations," pg. 27, 4/2010, <http://www.ewi.info/russia-us-bilateral-cybersecurity-critical-terminology-foundations>.

[17] Kim Zetter, "Condé Nast Got Hooked in $8 Million Spear-Phishing Scam," *Threat Level*, 4/4/2011, <http://www.wired.com/threatlevel/2011/04/condenast-hooked-by-spear-phisher/>.

[18] Steve Clayton, "Microsoft is Imagining a NUI future," Official Microsoft Blog, 1/26/2011, <http://blogs.technet.com/b/microsoft_blog/archive/2011/01/26/microsoft-is-imagining-a-nui-future-natural-user-interface.aspx>.

For the purposes of this paper, a cybercrime occurs when computers, networks and software are used to engage in criminal activity, and the victim of that crime is targeted through these electronic means.

That includes a wide swath of illicit activity. There are fake banking and social networking sites, designed to fool people into giving up their account numbers; a type of activity called "phishing." There are chains of infected computers—"botnets"—used to pump out mass e-mail comeons, among other criminal acts. Malicious software ("malware") is often used to take control of a machine and steal the information inside. There are the online equivalents of cat burglars, sneaking into corporate networks to pilfer company secrets. And there are shakedown artists who threaten web businesses with a flood of junk traffic if they do not comply with extortion demands.

The vast majority of online crime is relatively unsophisticated but brutally effective. Simple software makes identity theft almost idiot-proof; it was used to make off with $11 million from twenty businesses between March 2010 and April 2011.[19] Some of it is highly targeted and clever; for instance, the "spear phishing" scams that appear to come from the victim's friends or corporate customers. That is how Condé Nast managed to lose $8 million, almost in an instant.

A deeper infrastructure supports all of these activities, no matter what the complexity. Registration companies give phishers their realistic-sounding website domains. Hosting firms sell the server space and provide the Internet Protocol (IP) addresses that the botnet lord, the spammer, and the spear-phisher all need to make their wares online-accessible. ISPs are the gatekeepers to the broader Internet. Without these companies, none of these online crooks would be able to practice their trade.

This means that as vast and as complex as these criminal networks have become, there are nodes where they are vulnerable. There are places where they can be pressured to stop their activity or face prosecution.

[19] Internet Crime Complaint Center, "Fraud Alert Involving Unauthorized Wire Transfers to China," 4/26/2011, <http://www.ic3.gov/media/2011/ChinaWireTransferFraudAlert.pdf>.

Both Pirates and Privateers Online

These criminal tactics can be used separately or in combination, by skilled crooks or by neophytes. In an echo of the pirate heyday, there are signs that governments may be encouraging these crooks—and sharing technologies with them. In other words, there are both online privateers and online pirates roaming the criminal underground. And, as previously discussed, it's often hard to tell which is which.

In 2009, for instance, *someone* slipped into the extranets of leading American energy companies, stole executives' credentials, and used those passwords to exfiltrate billions of dollars' worth of information on oil deposits. The tools used to pull off the so-called "Night Dragon" break-ins were advertised on Chinese websites. The person who provided the hosting services for the caper was based in Shandong Province (although the servers themselves were on American soil). The people scouring the energy company networks "operated on a strict weekdays, nine-to-five Beijing time-zone schedule," according to a McAfee researcher.[20] Does that make Night Dragon a sophisticated criminal caper? An act of industrial espionage? A government-sanctioned operation? All of the above? If anyone knows for sure, they are not saying so in the open.

In public, U.S. officials do not usually identify specific network breaches as state-sponsored. Privately, however, those officials say that it's no accident that a worm used by Russian cybercriminals resulted in the biggest penetration of Defense Department networks ever.[21] They do not believe the apparent ties between a criminal-friendly hosting company in St. Petersburg and the local security services are coincidental.[22] Nor do they believe Beijing's protestations that that the Chinese government had nothing to do with so-called "Aurora" series of attacks, which targeted Google and at least 33 other companies in 2010. Joel Brenner, the former counterintelligence chief at the Office of the Director of National Intelligence, says that incident is just one example of many instances of China's "heavy-handed use of state espionage against economic targets."[23]

---

[20] Nathan Hodge and Adam Entous, "Oil Firms Hit by Hackers From China, Report Says," *Wall Street Journal*, 2/10/2011, <http://professional.wsj.com/article/SB10001424052748703716904576134661111518864.html?mg=reno-secaucus-wsj>.

[21] Private interview, 10/5/2010.

[22] Joseph Menn, Fatal System Error: *The Hunt for the New Crime Lords Who Are Bringing Down the Internet* (Public Affairs, New York, 2010), pg. 221.

[23] Brian Grow and Mark Hosenball, "Special report: In cyberspy vs. cyberspy, China has the edge," Reuters, 4/14/2011, <http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414>.

"I believe we are suffering what is probably the biggest transfer of wealth through theft and piracy in the history of mankind," Senator Sheldon Whitehouse, who chaired a classified task force on the subject, told his colleagues in 2010.[24]

[24] Congressional Record: July 27, 2010, Page S6265-S6266, <http://www.fas.org/irp/congress/2010_cr/cyber.html>.

"Cyberwar" vs. Cybercrime

While online crime—both simple and sophisticated, both government-connected and not—continues to rise, cybersecurity talk in Washington and in the popular press is dominated by dire predictions of a catastrophic cyber attack: an online "bolt from the blue" which sends networks crashing. Current and former top government officials claim that the United States is just a few clicks away from an electronic takedown of the banking system, the power grid or the Pentagon's command-and-control networks. "The United States is fighting a cyber-war today, and we are losing," retired Adm. Mike McConnell, the former director of the National Security Agency, declared last year.[25]

The references to "cyber 9/11s"[26] and electronic "Pearl Harbors"[27] are constant, and the scare-talk is echoed by an array of network security consultants. Events as trivial as the defacement of government websites—the digital equivalent of graffiti—are billed as the opening blasts of electronic Armageddon. Perhaps it's only coincidental that some of these alarmists stand to make money by responding to this crisis.

The cyberwar crowd has powerful allies in American defense policy circles. There, the Internet is sometimes presented as simply another "warfighting domain"—like the air or the sea, but made of 1s and 0s. Alternatively, the network of networks is viewed as a place to continue nuclear arms strategy. Both of those constructs may feel comfortably familiar to policymakers, but neither one comes close to describing the network security challenge.

Unlike nuclear weapons—held by just a few states, and technically difficult to obtain—digital attack tools can be possessed by anyone from criminal gangs to superpowers. Attackers (and defenders) can leap across national boundaries with a speed that would violate the laws of physics on the sea or in the air. Furthrmore, they can keep their identities largely hidden, even as they hop from place to place.

---

[25] Mike McConnell, "Emerging Risks: How to Win the Cyber-War We're Now Losing," 2/2/2011, <http://www.boozallen.com/insights/insight-detail/winning-cyber-war>.

[26] Senate Committee of Homeland Security & Governmental Affairs, "Lieberman, Collins, Carper Unveil Major Cybersecurity Bill To Modernize, Strengthen, And Coordinate Cyber Defenses," 6/10/2010, <http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=227d9e1e-5056-8059-765f-2239d301fb7f>.

[27] Jason Ryan, "CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor," ABC News, 2/11/2011, <http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905>.

The emergence of network attack and defense as an element of war presents enormous strategic concerns for the United States. The Pentagon's information security is spotty, as demonstrated by the relatively-simple worm that infected hundreds of thousands of Defense Department computers, (or the 18 months it took to clean those machines up).[28] Responsibilities in the event of a major strike on American networks are unclear[29]—a critical issue, given the vulnerabilities in the power grid highlighted by the Stuxnet worm. No one is sure where in cyberspace the "red lines" lie that would prompt a retaliatory attack; nor is it apparent what form that retaliation would take. Informal discussions are beginning to address these topics. But at the moment, there are no official dialogues on these matters between the two of the most likely network combatants—the United States and China.

The issue of network war presents a serious concern for the future. Meanwhile, the slow, rising tide of criminal activity is draining untold billions from the legitimate global economy *right now*. In 2009 and 2010, seven million U.S. consumers admitted to being tricked out of their personal information by online scam artists. Cybercrime losses reported to the FBI doubled from 2008 to 2009, to $559.7 million.[30]

Last year, the security firm McAfee detected an average of 60,000 new malicious software variants each day.[31] That is because it does not necessarily take technical skill to create malware anymore. For $1,500 or less, a novice thief can buy a copy of the Zeus or SpyEye crimeware kits. Either one will help the thief build a "Trojan"—a program that sneaks nefarious code onto a victim's computer. With a few mouse-clicks, the thief can configure what he wants his malware to do, which banking sites he wants to monitor, what information he wants to grab, and how to send that information back to him.[32] The interface to do it all is simple and if the thief gets stuck, the crimeware firms have reputations for fast, helpful customer service.

Crooks are paid as little as $.75 to install malicious software on an individual's machine—that is how simple it has become.[33] Victims do not even have to click to get infected; they just visit their favorite website, and malicious code embedded in the advertisement does the rest. Often, the victim's computer is chained together with tens of thousands of other infected machines to form "botnets." These arrays can then be rented for as little as $8.94 per hour,[34] allowing scammers and spammers to cheaply spew out millions of electronic come-ons.

Forget "Pearl Harbor"; if we are not careful, the Internet could become the equivalent of the South Bronx, circa 1989—a place of such rampant criminality that no one wants to live or do business there. As New Yorkers learned during those years, criminal acts, if sufficiently

---

[28] Noah Shachtman, "Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack," *Danger Room*, 8/25/2010, <http://www.wired.com/dangerroom/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/>.

[29] Noah Shachtman, "Military's Cyber Commander Swears: 'No Role' in Civilian Networks," *Danger Room*, 9/23/2010, <http://www.wired.com/dangerroom/2010/09/militarys-cyber-commander-swears-no-role-on-civilian-networks/>.

[30] Internet Crime Complaint Center, "2009 Internet Crime Report," <http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf>.

[31] McAfee, "A Good Decade for Cybercrime: McAfee's Look Back at Ten Years of Cybercrime," <http://www.mcafee.com/us/resources/reports/rp-good-decade-for-cybercrime.pdf>.

[32] Chintan Shah, "Zeus Crimeware Toolkit," McAfee Blog Central, 9/20/2010, <http://blogs.mcafee.com/mcafee-labs/zeus-crimeware-toolkit>.

[33] McAfee Security Journal, Fall 2008, <http://www.wired.com/images_blogs/threatlevel/files/mcafee_security_journal_fall_2008.pdf>.

[34] Matthew Broersma, "Botnet price for hourly hire on par with cost of two pints," *ZDNet UK*, 5/25/2010, <http://www.zdnet.co.uk/news/security-threats/2010/05/25/botnet-price-for-hourly-hire-on-par-with-cost-of-two-pints-40089028/?tag=mncol;txt>.

widespread, add up to an atmosphere of lawlessness that only encourages more criminality.[35] Today we are seeing a replay of that famous "broken windows" thesis—this time on our networks instead of on our streets.

Online crime might not be in the Washington comfort zone, as strategic arms are, but that does not mean the issue can be pushed to the margins. There is a long history of policymakers ignoring immediate-but-unconventional challenges in favor of familiar and theoretical ones. It rarely ends well.

[35] George L. Kelling and James Q. Wilson, "Broken Windows: The Police and Neighborhood Safety," *The Atlantic*, 3/1982, <http://www.theatlantic.com/magazine/archive/1982/03/broken-windows/4465/>.

A Surprising Partner

As cybercrime becomes increasingly more common, there is a growing constituency on both sides of the Pacific that is capable of working together against online crime syndicates. Despite all the network break-ins which seem to have their origins in China—and despite the Beijing government's alleged connections to some of these heists—the Chinese appear to be just as spooked about their online vulnerabilities as we are. According to one local report, "nearly all internal networks used by Chinese firms have been attacked at least once during the past year, and hackers managed to take control of at least 85 percent of them."[36]

In 2010, more than 45 percent of Chinese Internet users complained of viruses or Trojans on their computers, according to a recent study from the China Internet Network Information Center, which reports to the Ministry of Industry and Information Technology. Nearly 22 percent reported that their accounts or password had been stolen.[37] And that is actually an improvement over recent years. In 2009, the rate of infection was nearly 60 percent, and rate of account theft was almost one in three.[38]

The "country's aggressive cyber offense abroad," the security website *ThreatPost* notes, "is in stark contrast to an almost total lack of basic cyber defense at home." Beijing may sponsor online privateers, but it has also become easy prey to networked pirates. China's heavy reliance on unlicensed Windows software means that their operating systems do not receive regular security patches; their reluctance to embrace open source software means that "they do not benefit from the whole community of people who are crawling over those platforms and patching bugs and looking for holes," top security researcher Dillon Beresford observes.[39]

The sense of vulnerability is palpable. Beijing's network security officials have taken to publicly

---

[36] China.org.cn, " Net security proves difficult task," 3/12/2011, <http://www.china.org.cn/china/NPC_CPPCC_2011/2011-03/12/content_22120008.htm>.

[37] China Internet Network Information Center, "Statistical Report on Internet Development in China," 1/2011, <http://www1.cnnic.cn/uploadfiles/pdf/2011/2/28/153752.pdf>.

[38] Zhang Xiaojun and Liu Zan, "Internet safety calls for global cooperation," Xinhua News, 9/12/2010, <http://news.xinhuanet.com/english2010/indepth/2010-09/12/c_13491225.htm>.

[39] Paul Roberts, "Glass Dragon: China's Cyber Offense Obscures Woeful Defense," *ThreatPost*, 4/27/2011, <https://threatpost.com/en_us/blogs/glass-dragon-chinas-cyber-offense-obscures-woeful-defense-042711>.

calling China the "biggest victim" of cybercrime.[40] Others—like Gu Jian of the Ministry of Public Security's Network Security Protection Service—are asking for "closer, more effective cooperative relations with other countries in fighting against cross-border cybercrime." In a speech last November, Jian pleaded for the United States and China to cooperate more closely on criminal investigations, and establish "rapid coordination mechanisms" to resolve cases more smoothly.[41]

You do not have to take Jian wholly at his word—or pretend he speaks for the entire Chinese government—to see the possibilities for Sino-American cooperation against a common threat. Or to note that there is a somewhat similar alignment of interests in the Gulf of Aden, where Chinese and American warships are also looking to keep commerce flowing.

[40] People's Daily Online, "China 'biggest victim' of cyberattacks," 1/25/10, <http://english.peopledaily.com.cn/90001/90776/90883/6877232.html>.

[41] Gu Jian, "Strengthening international cooperation and joining hands in fighting against transnational cybercrime," China.org.cn, 11/9/2010, <http://www.china.org.cn/business/2010internetforum/2010-11/09/content_21306503.htm>.

Cybercrime First; Everything Else May Follow

The United States and China do not see eye-to-eye on a variety of topics. Yet the two sides cooperate on a whole range of issues—terrorism, child pornography and, yes, piracy. Even potentially combustible topics like intellectual property are sometimes tackled together through organizations like the "Joint Liaison Group for Law Enforcement Cooperation," led by the U.S. Departments of State and Justice and China's Ministry of Public Security. This group has driven several U.S.-Chinese cooperative investigations that have recovered millions of dollars in goods.[42] It's a lesson that governments do not have to agree on *all* things before they start cooperating on *some* things.

Of course, there are all kinds of unique obstacles to collaborating on cybercrime. The Chinese and American visions for the Internet are fundamentally different—one favors state control of networks, the other leaves them in the hands of private industry. The laws are different, especially the laws surrounding political speech and obscenity. Setting up working protocols between two countries, each with a dozen or more departments overseeing online commerce and crime, can be taxing. But it should not be as hard as it is. "The current cooperation between countries is abnormally inefficient," Jian notes. Talks around cybercrime should begin right away, to begin to resolve these issues.

RECOMMENDATION 1: BEGIN U.S.-CHINA TALKS, CENTERED AROUND CYBERCRIME
It's not just the most pressing issue; it's the one with the most common ground.

As an early topic, Jian suggests establishing guidelines for "cases of double criminality"—activities which are illegal both in America and China. It's a good suggestion; clarifying exactly which acts are legal and which ones are not for both countries could go a long way toward easing Sino-American tensions and marginalizing online crooks. Once those guidelines are set, the United States and China can move to tighten bilateral assistance agreements to collect evidence and run joint investigations on double-criminal cases.

A recent U.S.-China bilateral suggests a joint push against spam as a way to both build trust

[42] House Committee on Oversight and Government Reform, Subcomittee on Government Management, Organization, and Procurement, "Testimony of Deputy Assistant Attorney General Jason M. Weinstein on protecting intellectual property rights," 12/9/2009, <http://hongkong.usconsulate.gov/uscn_others_2009120901.html>.

and curb a global problem.[43] Eventually, China might even be persuaded to join the so-called "Budapest Convention" on cybercrime, which asks signatories, each in their own way, to take action against everything from network break-ins to online fraud to child pornography.[44]

Now this probably will not lead to investigations into China's alleged army of online privateers—its state-sponsored thieves and hijackers. But there are still benefits to working with Beijing to clamp down on the online pirates who are stealing from everyone. It helps U.S. consumers and businesses. And a dialogue on crime could begin to ease tensions over all sorts of Internet issues.

Such talks could establish the terms and working groups needed for more strategic topics. They could clarify the lines between online criminality and state-sponsored network breaches. And they could build momentum for military-to-military dialogues. In other words, cybercrime is the "low-hanging fruit" that might set the table for an entire diplomatic meal.

The Russian, American and Chinese governments have widely different stances on whether network exploits can or should be used as tools of war. But robberies, break-ins and con games—those are different. There is no public constituency for cybercrime.

The Chinese (and others) may be accused of employing the unsavory to carry out strategic-level intellectual property theft. The Russians could be masking the signal of espionage with the noise of crooks. That only adds to the urgency of coming to a better understanding on crime. Stripping away the cybercrooks could expose the online spy—and perhaps undermine his actions as well. Here's why: it is not uncommon today for a network security team at a big U.S. company to spend 80 percent of its time on rudimentary, if pervasive, criminal infiltrations—the online pirates, if you will. Slowing these break-ins could free up those teams to concentrate on the higher-end, possibly state-sponsored swath of cybercrime: the online privateers. What is more, sophisticated criminals often use simple tools in order to hide themselves in the swarm of everyday infiltrations. If there were fewer of these run-of-the-mill attacks, the online privateer might have a harder time keeping his identity cloaked.[45]

In the 19th century, a global agreement to ban privateering set the stage for a dramatic reduction in piracy on the high seas. This time around, the practice might work in reverse: focus on the average, independent cybercrooks first, and then tackle the ones who are state-sponsored.

RECOMMENDATION 2: DRAW THE CHINESE INTO THE LARGER COMMUNITY OF ISPs AND NETWORK CARRIERS.
It should speed the resolution of major network issues—and encourage China to become a more responsible actor on the global network stage.

The most fruitful conversations will not necessarily be government-to-government—or, at least, they will not end up that way. As mentioned above, the Internet is really a collection of a few thousand networks, almost all of which are in private hands. Most of the people who provide access to those networks are in regular touch about common threats and technical issues. Today, China's Computer Emergency Response Team and its ISPs are nothing but e-mail addresses to the wider Internet community. There is no one person who consistently answers that address or

[43] Karl Rauscher and Yonglin Zhou, "Fighting Spam to Build Trust," East-West Institute., 5/27/2011, <http://www.ewi.info/fighting-spam-build-trust>.
[44] Council of Europe, "Convention on Cybercrime," 11/23/2001, <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>.
[45] Private interview, 5/20/11.

returns messages with any sort of predictability. There is no one with whom a working relationship can be established. In a network of networks that relies almost exclusively on informal agreements and good faith, this situation is less than optimal. It not only keeps China at the edges of the global network ecosystem, it severely limits the ability of the entire ecosystem to push out the worst-of-the-worst criminal actors—to get rid of the crooks who are preying on both Chinese and American networks. So the first goal of any talks should be to encourage China to have a consistent presence in the global community that makes the Internet work.

Who Gets Squeezed?

Last July, former National Security Agency Director Michael Hayden mused about one negotiating strategy with a country like China or Russia. He suggested punishing the states that harbor online crooks. "Since… it's difficult to prove state sponsorship, one of the thoughts … is to just be uninterested in that distinction and to actually hold states responsible for that activity emanating from their cyberspace," Hayden told the Black Hat hacker conference.[46] Others in U.S. policymaking circles have floated the idea of slowing down or cutting off Internet traffic from, say, China, if their online crooks and spies will not leave us alone. Lt. Commander Matthew Sklerov, writing in *Military Law Review*, counsels the United Sates to "hold sanctuary states responsible for violating their duty to prevent cyberattacks."[47]

This may be too literal an interpretation of the anti-piracy precedent. The business ties between America and China are so strong these days that a national-scale Internet block would punish both of our economies. (Besides, a blockade is an act of war.) The ability to route traffic through a dozen different states, lease server space in a dozen others, and form alliances with cybercrooks-for-hire elsewhere makes it tough to tell where the criminals are really coming from; countries could get blamed for attacks over which they have very little sway.

RECOMMENDATION 3: AVOID NATIONAL RETALIATION AS A CYBERCRIME SOLUTION.
It is too blunt an instrument for the nuanced issue of cybersecurity; besides, many of the worst criminals set up shop in the United States.

The Internet is mostly a collection of businesses, not a collection of governments. For all its flaws, this is a system that fundamentally works —witness the relentless double-digit annualized growth of the Internet. Inserting additional national controls into this arrangement is something to be resisted, not embraced.

But if a country-wide block is too blunt an instrument to be useful, there are more precise tools

[46] Kim Zetter, "Former NSA Director: Countries Spewing Cyberattacks Should Be Held Responsible," *Threat Level*, 7/29/2010, <http://www.wired.com/threatlevel/2010/07/hayden-at-blackhat/>.
[47] Matthew Sklerov, "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent," *Military Law Review*, Volume 201, Fall 2009.

that could be employed. A relative handful of firms provide the infrastructure for a huge swath of the cybercriminals worldwide. The networks of just 50 ISPs account for around half of all infected machines worldwide, according to a study prepared for the Organization for Economic Cooperation and Development.[48] A tiny portion of the world's registrars regularly service criminal clientele. Just three firms process 95 percent of the credit card transactions for the drugs and herbal remedies advertised by spammers.[49] A small minority of hosting companies caters to crooks. When one particularly noxious hosting company—McColo Corp. of San Jose, California—was taken down, the volume of spam worldwide dropped by 70 percent.[50]

These companies are in business with, and accessories to, criminal enterprises. And, unlike the criminals themselves—who hide behind disposable e-mail addresses, anonymously-registered domains and encrypted communications—it's no mystery who these firms are. The independent research group HostExploit, for example, publishes a quarterly list of the worst-of-the-worst hosting companies and networks.

RECOMMENDATION 4: LEAN ON THE CRIMINAL SUPPORT NETWORKS.
Online crooks depend on these businesses. That makes them nodes of pressure and of vulnerability.

So any pressure is better applied not on nation-states, but on this larger ecosystem that abets criminality. Blacklist the payment companies that funnel money to the spammers, for instance, and you very well may undercut the spammers' reason for sending out bulk e-mail in the first place. The criminal cannot commit his crimes without these business partners. Therefore, "affecting (or threatening to affect) those relationships can influence the behaviors of an actor; and it should be generally applicable to forestalling a wide range of potential threats," writes SAIC's Jeff Cooper.[51]

That might seem like a relatively straightforward proposition. Internet providers merely have to be convinced to pull the plug on their most felonious hosting customers. Most of the big "tier 1" networks already forbid spam, computer takeovers, and other criminal activities in their user agreements. They are well within their rights to disconnect those crooked hosts.

But the ISPs rarely exercise those rights. McColo was only "depeered" by its ISPs after the journalist Brian Krebs and others spent months assembling data that finally persuaded the providers to disconnect the crime den.[52] Limestone Networks out of Dallas, Texas spent four years on HostExploit's list of the world's 50 most criminal-friendly hosting companies (out of more than 47,000).[53] Until recently, Limestone hosted the command-and-control servers for Coreflood, one of the oldest and biggest botnets of all time. Yet no action has been taken against Limestone, despite the associations.[54]

In the 17th century, the town of Port Royal, Jamaica became an infamous pirate paradise. There, hijacked goods were sold, crews recruited and raids launched along the trade routes. Governments

---

[48] Van Eeten, et. al.
[49] Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, et. al., "Click Trajectories: End-to-End Analysis of the Spam Value Chain," IEEE Symposium on Security and Privacy, May, 2011, <http://cseweb.ucsd.edu/users/klevchen/lpcefghkklmwpvs-oakland11.pdf>.
[50] <http://www.informationweek.com/news/security/vulnerabilities/216401850>.
[51] Jeffrey Cooper, "New Approaches To Cyber-Deterrence: Initial Thoughts On A New Framework," December, 2009.
[52] Brian Krebs, "Major Source of Online Scams and Spams Knocked Offline," *Security Fix*, 11/1/2008, <https://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html>.
[53] Sitevet, **"AS46475,"** <http://sitevet.com/db/asn/AS46475>.
[54] HostExploit, "CoreFlood Hosting," 4/19/2011, <http://news.hostexploit.com/hosts-and-registrars-news/4864-coreflood-hosting.html>.

not only knew what was happening there—they turned a blind eye to the hijackers and their haven. It is easy to imagine an outfit like McColo as the 21st Century equivalent. Eventually, Port Royal was brought down by an earthquake. We will not be so lucky with its online analogues. The rest of the Internet community will have to do the job.

It is Up to the ISPs

Unfortunately, some of the companies best positioned to interrupt the cybercriminal ecosystems are the ones with the least incentive to do so.

There is a long-standing aversion in the ISPs to policing the content that travels on their networks. Besides, there is not much of a direct economic benefit for an ISP to turn aggressive against cybercrooks. Even crime-ridden hosting companies have legitimate customers, too, and all of those downstream customers—illicit and not—ultimately pay for the Internet access that the ISP provides. If an ISP gets overly aggressive with those customers, its bottom line could suffer quickly.

What is more, while the ISP may have a criminal enterprise based on its network, the victims of those crooks may be on some other network, or in another country, so there is no real harm to the ISP.[55]

Along with that economic disincentive, there is also an information gap. ISPs are disinclined to look for individual infections on their network; the investigations can be intrusive, and the clean-ups costs high. This means the true costs of the overall cybercrime problem remain hidden—and the pressure to act against the problem is eased.

When ISPs' direct financial interests are at risk, however, they have proven to be more than willing to filter, block, or redirect traffic. And the information about threats flows freely. All of this is done regularly to defend against Distributed Denial of Service (DDOS) attacks. In a DDOS, compromised computers are used to overload servers with so many requests for information that the machines collapse. DDOSs can generate enormous amounts of traffic—as much as 50 gigabits per second. The traffic is not only expensive for an ISP to haul—the capacity to handle that much data on a monthly basis might cost $50,000 on the open market—it can also threaten the connectivity of a whole range of ISP customers while a particular victim gets pounded. So ISPs have to pay for maintaining excess bandwidth in case they get hit.

Many large ISPs—and many Internet Exchange Points, which provide even higher-level connectivity—have joined together in a group to limit attacks like these. When a DDOS grows into something substantial, the group members distribute lists of Internet Protocol addresses to block and digital filters to keep the traffic out. They even, in rare cases, turn the traffic back on a repeat attacker.

[55] Moore (2010)

This is all made easier because there is no need to examine the content of that traffic—just the data's flow—and because the ISPs hosting attacker and victim alike have to bear the costs of that excess bandwidth. Even so, the results are startling: A serious attack is mitigated two to five times per day.[56]

RECOMMENDATION 5: MOTIVATE ISPs TO PRESSURE THE CRIMINAL ECOSYSTEM.
They are perfectly placed to interrupt illicit traffic.

So the question is how do you motivate ISPs to work like this to stop other kinds of online crime? How do you give these companies some sort of financial incentive for rooting out botnets and the like? Finally, how do you encourage ISPs to begin to share data on these threats with one another?

[56] Private interview, 4/21/2011

A "Grand Bargain" For Security

One method is simply to fine the ISP that does not immediately disinfect the machines on its network. In a report for the European Commission, Anderson et al. suggest that the provider get hit with a "fixed penalty" for "machines that continue to misbehave after a reasonable duration, say 3 hours," after notification of the infection.[57]

It is a crude solution to a problem as wide-ranging as cybercrime. Some malware is easy to find; some is hard. Some malware is easy to remove; some is not. That undercuts the idea of a one-size-fits-all fine for every missed infection. The proposal also treats the master (the botnet controller) and the slave (the hijacked machine) similarly, when one is a clearly more damaging entity than the other. Furthermore, the fixed penalty could be seen as a disincentive for ISPs to share—or even look for—evidence of cybercrimes. Why search if all you're going to find is potential fines?

A second method goes in the entirely opposite direction, subsidizing the ISPs' disinfections. Moore proposes a clean-up fund, jointly backed by the government and the major software companies. Which firm pays depends on which program was used to compromise the machine. The government pays for the open source efforts.[58] In return, the government gets a more efficient, better-connected economy and the software makers avoid any possible lawsuits that the infected machines might generate.[59]

Moore casts the fund as part of "grand bargain" between software companies, the government, and Internet providers. It involves more than giving ISPs a financial incentive to keep their networks clean. It would also hold ISPs liable for damages if they did not disinfect machines quickly.

As Douglas Lichtman of the University of Chicago notes, it's not unusual for an offline business to be liable for damage it may not have directly caused. That is particularly true if that company could've done something to deter that bad act.[60] A retailer can be culpable if its delivery van hits

---

[57] Ross Anderson, Rainer Böhme, Richard Clayton, and Tyler Moore, "Security Economics and European Policy," 2008, <http://www.cl.cam.ac.uk/~rja14/Papers/enisa-short.pdf>.

[58] Moore (2010).

[59] Michael L. Rustad and Thomas H. Koenig, "The Tort Of Negligent Enablement Of Cybercrime," *Berkeley Technology Law Journal*, 20.4: 1553-1611, Fall, 2005, <http://www.law.suffolk.edu/faculty/addinfo/rustad/rustad.koenig.final.pdf>.

[60] Douglas Lichtman, "Holding Internet Service Providers Accountable," *Regulation*, Winter 2004-2005, pgs. 54-59, <http://www.cato.org/pubs/regulation/regv27n4/v27n4-7.pdf>.

someone and the company did not properly service the vehicle. Landlords are deemed accountable if they do not put locks on their doors and burglars walk in.' Similarly, both Lichtman and Moore argue, ISPs cannot just allow criminal havens to linger on their networks.

Avoiding the liability is seemingly easy under Moore's plan: just clean up customer machines as soon as you're notified of an infection. Moore models his plan on the Digital Millennium Copyright Act, which forces providers to comply with copyright holders' demands to take down any pirated music, movie, software, image or service.

Moore's plan represents the most comprehensive attempt yet to get the best-placed parties to curb the most prevalent form of online crime. It should not be dismissed lightly, but it does have at least three weaknesses.

First, its model—the Digital Millennium Copyright Act—is notoriously open to abuse. Technology news service Ars Technica had its Facebook page removed after a single vague e-mail.[61] A speaker wire company sued a search engine that included its cables in the search results.[62] The list is as endless as it is asinine. And no wonder: under DMCA, anyone can issue a takedown notice, forcing a company to comply or risk a legal battle.

Another potential issue is Moore's idea that software firms have to fund malware clean-ups or face lawsuits of their own. There are real questions about which companies would be forced to participate—beyond the obvious players like Microsoft and Adobe—and what looming penalties will do to innovation in the software sector. As Harvard's Jonathan Zittrain notes, today's computing environment is a "generative" one; the latest programs leverage the code that came before them. Any sufficiently popular product these days gives rise to a whole family of new software. Just look at the hundreds of thousands of programs in the iPhone and Android app stores. Introducing legal threats into that environment "would serve only to propel PC lock- down," stifling the buzz of generative creativity.[63] There is universal agreement that software firms ought to be paying more attention to security as a first principle as they write their code, but penalizing them if they leave a buffer overflow is an idea that ought to be considered very cautiously.

However, the biggest shortcoming with Moore's "grand bargain" may be that it ignores one of the most toxic components of the online crime formula: the hosting company supporting a criminal gang. Under Moore's plan, ISPs are suddenly liable for cleaning up countless millions of infected machines—the victims of cybercrime, essentially—while a relatively small number of crooks are allowed to roam free. It is like focusing on exclusively door-locking, instead of on the robbers poised to kick those doors in. Both are important, but a motivated crook is always going to be able find a way in.

As Moore himself finds in a forthcoming paper, "countermeasures that block malicious transit traffic appear more effective than ones that block outgoing traffic... Our results also suggest that when only the largest ASes [autonomous systems—hosts and ISPs] intervene, it is better to simply filter out malicious traffic... than to attempt to remediate end-user infections."[64]

---

[61] Ken Fisher, "Facebook shoots first, ignores questions later; account lock-out attack works," *Ars Technica*, 4/28/2011, <http://arstechnica.com/business/news/2011/04/facebook-shoots-first-ignores-questions-later-account-lock-out-attack-works.ars>.
[62] Mike Masnick, "Monster Cable Issues Yet Another Bogus DMCA Notice To A Search Engine," *TechDirt*, 1/10/2011, <http://www.techdirt.com/articles/20110109/21155712581/monster-cable-issues-yet-another-bogus-dmca-notice-to-search-engine.shtml>.
[63] Zittrain, Jonathan, The Future of the Internet—And How to Stop It (Yale University Press, New Haven, CT, 2008) pg. 162.
[64] Tyler Moore,"Modeling Internet-Scale Policies for Cleaning up Malware" (forthcoming).

One Proposal for Pressuring the Criminal Ecosystem

That is why Moore's model should be turned on its head. The focus ought to be on punishing the businesses at the heart of the cybercriminal ecosystem—the hosting companies and the platforms they need to pull off their scams and robberies. It is those firms that should be vulnerable to legal action if they continue to support criminal enterprises.

RECOMMENDATION 6: HOLD THE WORST HOSTING COMPANIES LIABLE FOR THEIR CRIMINAL CLIENTS AND THE WORST ISPs LIABLE FOR THEIR CRIMINAL HOSTS.
This will provide financial incentives to turn against the criminals, instead of profiting from their traffic.

Here's a sketch of how it might work:

- First, an outside agency is deputized to maintain a list of the hosting companies with the closest ties to crime. For the moment, let us say it is HostExploit's quarterly list of the 50 worst. But it could also be maintained by a number of security specialists, or a combination of them all. The list would rely on a transparent methodology, so that everyone involved could see which specific activities were most problematic to the wider community. The methodology would have to conform to a global consensus about what constituted criminal behavior. No single government, in other words, could brand a particular firm as an outlaw.
- Once the roster is published publicly, a listed company would have fourteen days to either drop their illicit customers or to explain why it does not belong on this roll of the worst-of-the-worst. If the company complies (or explains itself sufficiently), then it is granted safe harbor from any lawsuit that might arise from the harm generated by the spammers, phishers and botnet herders it once helped.
- If the hosting company fails to comply, however, it becomes subject to a liability lawsuit. The company has already been warned that it's facilitating harmful activities and given a chance to correct its negligent behavior.
- If that same company ignores the warnings and appears on the worst-of-the-worst list for a second quarter, the firm's ISP should also be liable. (Of course, the provider should be given at least as much time and opportunity to address the problem.)

Such a system gives ISPs enormous incentives to disconnect bad hosts, even if it means a temporary dip in revenue. This plan provides a clear standard for bad behavior, and a clear path for leaving the rogue's gallery. Most importantly, perhaps, it applies pressure on the broader ISP community to weed out the worst-of-the-worst – without heavy-handed government intervention.

"In all of the notable eras of piracy," University of South Carolina historian Donald Puchala writes, "relationships between pirates and those who abetted their projects amounted in effect to conspiracies of greed. The relationships were symbiotic: pirates could neither accomplish their ends nor convert their booty into profits without the aid of their protectors; for their part, the protectors could not so readily and splendidly enrich themselves without the booty brought in by the pirates." Cities like New York, then a British colony, grew fat off of pirate riches.[65]

One of the turning points in global attitudes toward piracy occurred when pirates began to threaten the economic interests of the states that previously sponsored them. The pirates picked fights with allies, hijacked friendly ships, and, as a result, made new enemies in cities like London and Paris.[66] And when the governments decided to definitively retaliate, one of the first steps they took was to shut down the markets for pirate booty. The most effective way to target the hijackers was through their economic support system.

We now may be at a point of a similar shift online. If ISPs start seeing rogue hosting companies as financial time bombs instead of as paying customers, it would represent a huge step forward in marginalizing cybercriminals globally. The threat of liability lawsuits could well provide the impetus for that shift.

In order for the plan to work, however, it has to be crystal clear. Companies on the worst-of-the-worst list need to know exactly how they got on the roster, and exactly what they need to do to get off it. The firms should be given ample time to resolve the issues that got them off the worst-of-the-worst roster. Some of the bills making their ways through Congress currently do not have those protections; anyone can sue anyone at any time, apparently. And that is wrong. As Google General Counsel Kent Walker recently told Congress, "Legislation should not include a private right of action that would invite suits by 'trolls' to extort settlements from intermediaries or sites who are making good faith efforts to comply with the law."[67]

To avoid that possibility, the illicit activities contributing to a company's placement on that roll have to be limited to a few universally recognized crimes: theft, fraud, and criminal trespass, for example. Politically inflammatory speech and even copyright infringement have to be left off of the list; they are too open to abuse and overly broad interpretation.

Neither the United States, nor any other government, should get into the business of picking which companies are in this rogues' gallery, but Congress may need to act before a plan like this could be put into action internationally. Liability and negligence are generally well-charted territories of the law. The legal maps specifically for hosting companies and ISPs' liability are less detailed.

There have not been many lawsuits against these firms for negligence. Exactly who would have the

---

[65] Donald Puchala, "Of Pirates and Terrorists: What Experience and History Teach," in *Contemporary Security Policy*, Vol.26, No.1, April 2005, pg. 9.
[66] Thomson, pg. 109.
[67] Kent Walker, "Testimony before the the House Judiciary Subcommittee on Intellectual Property, Competition, and the Internet," 4/6/2011, <http://judiciary.house.gov/hearings/hear_04062011.html>.

standing or the incentives to file these suits is murky. The precedents are, at best, confusing. In *Green vs. America Online*, the U.S. Court of Appeals found that the Internet provider was "statutorily immune from liability from causes of action arising from third party content."[68] By contrast, in *Arista Records LLC v. Lime Group LLC*, a U.S. District Court found that a peer-to-peer network was liable for copyright infringement, because the network was aware of widespread infringement by its users and did not take "meaningful steps" to stop it.[69] The Digital Millennium Copyright Act states that ISPs are liable when they are given notice of infringement on their network—but before that notification comes, the firms are not liable at all. Harmonizing these seemingly contradictory rulings may "require a government mandate to work," Harvard's Jack Goldsmith notes.[70]

Even with such a mandate in place, this plan will not help in all cases. There may not be much to be done, for example, when criminals use otherwise-legitimate hosting services as a launch pad for their attacks. Another roadblock: so-called "bulletproof hosting" services, which promise to keep customers' content online no matter how many threats or complaints are received. Those hosts are even more bulletproof when they are located overseas. As Kirill Levchenko, with the University of California, San Diego observes, the supply of hosting resources is vast, and the costs of switching providers is low.[71] In other words, occasionally punishing a single host from time to time will not work. Instead, the rules of the hosting game have to be tweaked, to make the supply of server space to criminal enterprises a more dangerously and costly proposition.

Many of these criminally-friendly firms may remain beyond reach of a lawsuit, based in places like China and Russia.[72] Some of the most venomous cybercrime crews are based in these counties. Still, the United States is not such a bad place to begin a global push against cybercrime havens. Twenty of HostExploit's 50 worst are American firms; only five are Russian, and three are Chinese.[73] By some measures, the United States is the planet's leading home for illicit Internet activities like spam and phishing, with three times the spam havens as China and more than twenty times the phishing sites. (Some of the spammers and phishers themselves may be based abroad, but they are taking advantage of America's relatively laid-back approach to cybercrime law enforcement to set up shop here.)

Even overseas and supposedly-bulletproof hosts are susceptible to pressure. These companies have limited customer bases, and are prone to extortion schemes from other criminals. The firms also have limited ways to get paid for their gray market services. Squeeze those moneymen, and the bulletproof hosts become vulnerable.[74]

Besides, more aggressively targeting the criminal ecosystem in the United States not only helps protect American consumers, it also allows America to lead on a vital issue. History has shown that when America makes changes to its own laws, countries worldwide often follow suit.

---

[68] Green v. America Online (AOL), 318 F. 3d 465 - Court of Appeals, 3rd Circuit, 2003, <http://scholar.google.com/scholar_case?case=10721627510353693908&hl=en&as_sdt=2&as_vis=1&oi=scholarr>.

[69] Arista Records LLC et. al. vs. Lime Group LLC et. al. 06 CV 5936 (KMW) U.S. District Court, Southern District of New York, 2010 <http://www.wired.com/images_blogs/threatlevel/2010/05/limewireruling.pdf>.

[70] Jack Goldsmith, "Senator Cardin's Bill to Explore ISP Enforcement of Digital Security," *Lawfare*, 12/9/2010, <http://www.lawfareblog.com/2010/12/senator-cardin%E2%80%99s-bill-to-explore-isp-enforcement-of-digital-security/>.

[71] Levchenko, Pitsillidis, Chachra, et. al.

[72] Brown, Cummins, Greathouse, et. al.

[73] HostExploit, "Top 50 Bad Hosts & Networks 2011 Q1," 4/14/2011, <http://hostexploit.com/downloads/viewdownload/4-reports/29-top-50-bad-hosts-a-networks-2011-q1.html>.

[74] Jonathan Brown, Amnda Cummins, Erin Greathouse, et. al., "A Preliminary Study of the Bulletproof Hosting Landscape," 4/23/10, <https://www.infosecisland.com/blogview/4487-Bullet-Proof-Hosting-A-Theoretical-Model.html>.

"Many international norms began as domestic norms," Martha Finnemore, the international relations theorist, writes.[75] A trend started at the beginning of the Republic. The groundbreaking U.S. Neutrality Act of 1794 forbid American citizens from forming or joining "military expeditions against a state with which the United States is at peace." In the years that followed, 49 other countries signed similar prohibitions, setting the stage for a two century-long decline in mercenarism and piracy.[76]

[75] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization*, Vol. 52, No. 4, Autumn, 1998, pgs. 887-917.
[76] Thomson, pgs. 78-82.

Protecting the Victims

Pressuring the criminal support networks alone will not be enough to curb cybercrime. More will have to be done to secure the individual users being targeted by the phishers, the spammers, and the botnet herders. Again, ISPs, who sit between those users and the open Internet, will likely find themselves with additional responsibilities.

RECOMMENDATION 7: ENCOURAGE ISPs TO NOTIFY CUSTOMERS OF INFECTIONS. *It is easy for the providers to tell which clients have been compromised, and it is better for everyone if those breaches get fixed.*

A number of intriguing approaches have been tested and proposed in the last eighteen months to make it as painless as possible for ISPs to guard against attacks, while still providing some relief to consumers. One answer is to make it very, very cheap. That is the model of a voluntary Australian program—set up by the local ISP industry itself.

Under the so-called "iCode" program, the Australian government looks for signs of botnets, and then hands out what it finds to the ISPs in daily reports. The government finds about 19,000 newly-suspected machines per day. The ISPs then choose to respond in the way they feel is best. In most cases, they notify customers with a phone call or an e-mail. In the more extreme cases, the ISP might confine the customer to a "walled garden," in which Internet access is severely limited until that person cleans up his or her machine.[77]

There is no public data, yet, on how the iCode program is doing; it's only been up and running for a few months. But iCode has proven so lightweight, and so easy to accept, that all of the country's major ISPs—covering 90 percent of the market—have joined in the voluntary effort. Which means that for the first time, the vast majority of Australians will now be notified if their machines get infected.

The program, however, is so lightweight that it may not work as a model for American action. End users are left holding the bag for cleaning out their computers, when they may not have done anything to bring about the infection and may not have the skills to get rid of the malware. Meanwhile, the government takes on the job of botnet monitor-in-chief. The temptations to turn that into a multi-purpose surveillance role might be too great to ignore. Besides, this practice runs

[77] Private interview, 4/18/11.

counter to stated American policy. As President Obama said in 2009, "Our pursuit of cybersecurity will not—I repeat, will not—include monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans."[78]

An American ISP, Comcast, is piloting a second approach, with a program called "Constant Guard." The security firm Damballa hunts for botnet traffic, primarily by combing through Domain Name Server data—the information that translates a name ("website.com") into a series of numbers called an Internet Protocol address. Damballa provides Comcast with a list of botnet servers, and the IP addresses of customers communicating with those servers. Comcast notifies the infected customer, who is then offered a range of security options, from antivirus software to technician support, to clean up the infection remotely.[79]

As in the Australian case, Constant Guard is too new to provide meaningful results; it has only been fully up and running since early April. Comcast sees the security enhancements as a potential competitive advantage in an ISP marketplace that is growing more crowded. Since it requires only a few people to operate, Constant Guard was fairly cheap to implement.

Compared to the Australian plan, there are fewer civil liberties concerns. Customers can opt out of the program, and Comcast is only looking to see if a customer's machine is reaching out to a botnet server—not at the actual content of the customer's communications; the government is not involved.

Whichever model is adopted—iCode, Constant Guard or something else—the government should encourage ISPs to start notifying their customers of infections on their machines. If the service providers agree to do this voluntarily, fine. That would be preferable to some government mandate.

RECOMMENDATION 8: AMEND THE LAWS TO ALLOW ISPs TO SHARE ATTACK DATA.
Spotting criminal trends early requires more information.

iCode does have one distinct advantage over the American project: it includes all of the major Australian ISPs who get a common, daily-updated data feed. Comcast keeps the ConstantGuard data to itself. With crooks hopping to new domains, using hosts and deploying new malware seemingly every second, that compartmentalization impedes efforts to corral online crime. It is not even possible to get a sense of the true scope of the cybercrime problem unless all the major ISPs share what they find.

At the moment, however, it is unclear if it would be legal for the providers to share information. There are antitrust issues to consider when competitors pool information. And while the Electronic Communications Privacy Act of 1986 plainly permits an ISP to monitor communications for the protection of its own network,[80] it's less obvious whether or not the act allows a provider to share that data with other companies.[81]

Some ISPs get around this barrier by allowing independent security firms like Damballa to

---

[78] Barack Obama, "Remarks By The President On Securing Our Nation's Cyber Infrastructure," transcript, <http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/>.
[79] Private interview, 5/4/11.
[80] Comments of the Center for Democracy and Technology, In the Matter of Cybersecurity, Innovation and the Internet Economy, Docket No. 100721305-0305-01, 9/20/2010, <http://www.nist.gov/itl/upload/Center-for-Democracy-and-Technology_Cybersecurity-NOI-Comments_9-20-10.pdf>.
[81] Aaron Burstein, "Amending The ECPA To Enable A Culture Of Cybersecurity Research," Harvard Journal of Law and Technology, Volume 22, Number 1, Fall, 2008 <http://jolt.law.harvard.edu/articles/pdf/v22/22HarvJLTech167.pdf>.

monitor their networks. These firms trade some information—like new malware variants—to then secure the rest of their clients. But the security firms also keep a great deal of information to themselves. Damballa, for instance, does not tell its customers what it is finding on other customer networks, except in the most general way.

That is why some have proposed carving out a limited antitrust exemption for security issues for ISPs, much in the same way the Year 2000 Information and Readiness Disclosure Act of 1998 allowed for the pooling of data about Y2K vulnerabilities.[82] ECPA may also need to be amended so that these Internet providers can share data on botnets and other criminal activities directly—as long as that data is first anonymized to protect consumers' personal information, and as long as users can opt out of the project.

[82] Larry Clinton, "Cyber-Insurance Metrics and Impact on Cybersecurity," White House Cyberspace Policy Review, 3/29/2009, <http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cybersecurity.pdf>.

Corporate Responsibility

The circle of disclosure and accountability should expand far beyond ISPs. Businesses must tend to their corporate networks—and share what they find—just as ISPs are supposed to take care of theirs. In the 19th century, it was up to the nation-state to clamp down on piracy by establishing responsibility over their territories. In the 21st century, it is up to government to provide private companies with the proper incentives to exercise the same type of authority and accountability.

But some of the same disincentives that inhibit ISPs' data-sharing and disinfection hold back these businesses as well. The compromised machines on a company's network may be targeting computers at some other corporation; so the real harm is felt elsewhere. And because the true scope of cybercrime remains a mystery, executives have a hard time figuring out how much to spend to defend their networks.[83]

Perhaps more important are the perceived competitive concerns. In boardrooms and in corporate IT departments, the flaws (or strengths) of a corporate security system are seen as vital trade secrets. Disclose too many infections, so the logic goes, and those secrets get spilled—maybe to a competitor, maybe to another crook. Why take that risk?

There are liability concerns too. Some security consultants say they have offered corporations lists of infected machines on their networks—only to have those lists rejected because the companies worried that with knowledge came culpability for what those computers did.[84]

Hoarding this data ignores one of the biggest security lessons of the last quarter-century: criminal data becomes more powerful as it's aggregated and analyzed. As police departments learned during the urban crime reductions of the 1990s and 2000s, what may appear at first glance to be an isolated break-in at a convenience store can turn out to be a part of a city-wide spree. That kind of information helps police deploy resources more efficiently, identify suspects faster and put felons in jail for longer.

It is a lesson learned long ago by the big antivirus firms, like McAfee and Norton. When one security company finds a new malware variant, that

[83] Anderson et. al. (2008).
[84] Private interview, 3/8/11.

company shares it with the other security vendors. It is the only way the security companies can hope to keep up when there are tens of thousands of new malware signatures appearing every day.

This also shows that sharing threat information does not have to be some sort of competitive handicap. After all, if these companies—*whose core business is security itself*—can manage to pool their data without harming their bottom lines, surely firms in other sectors can manage to do the same.

Various industries—information technology, financial services, and public transit, to name a few—have set up "information sharing and analysis centers" where security specialists are supposed to trade threat data and best practices for network defense. These centers are supposed to share with one another and, eventually, with the government. But the performance of these groups is wildly uneven and their proceedings are often kept private, even classified.

So for the most part, data-sharing continues to be an ad hoc affair—dependent as much on whom a security officer knows as how important the information is. Even top criminal researchers at Microsoft—who presumably have more information available about more people's desktops than anyone—still rely on word-of-mouth information and their social networks to learn about emerging criminal threats.[85]

The consequences of keeping quiet about breaches can be devastating. In the fall of 2008, for example, online thieves based in China broke into the networks of three of the world's biggest energy companies and stole some of their most important proprietary information: the details of their oil discoveries. The value of that information is valued in the billions of dollars, but the firms did not realize the full extent of what had happened until the FBI informed them at a meeting in 2009.[86] The oil men had not told each other about the breaches.

A few months later, a new round of intrusions began, this time targeting the energy companies' bidding information. By then, several executives at the largest companies had begun sharing network attack data. They saw that the infiltrators all used the same techniques to gain access to corporate directories, the same software to control company computers remotely, and the same pathway to send information back to China.[87] Within four months, they had the pattern down—and the tactics to counteract it. Many smaller companies, however, were out of the loop. They did not find out what had happened until McAfee published a research paper—two years after the attacks had begun.[88]

RECOMMENDATION 9: PUSH COMPANIES TO EXPAND REPORTING OF NETWORK BREACHES.
It is good for consumers; it may shame some firms into shoring up their networks; and it provides more data for cybercrime detection.

A number of proposals are circulating in Congress and among policymakers to compel companies to share more about their network breaches and criminal threats.

---

[85] Private interview, 4/29/11.
[86] Mark Clayton, "US oil industry hit by cyberattacks: Was China involved?," *Christian Science Monitor*, 1/25/2010, <http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved>.
[87] McAfee Foundstone Professional Services and McAfee Labs, "Global Energy Cyberattacks: 'Night Dragon,'" 2/10/11, <http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>.
[88] Private interview, 5/11/2011.

One idea, as discussed previously, is to carve out antitrust and ECPA exemptions for certain kind of security-related information. A second is to require public companies to discuss major network breaches in a Form 8-K for the Securities and Exchange Commission, which advises stockholders of unscheduled and material events. Under the plan, companies would also inform shareholders about the state of their network security under the "risks" section of its annual 10-K reports.

This requirement does not have to involve any new laws or regulations; in fact, it is already on the books, Senate Commerce Committee chairman Sen. Jay Rockefeller believes. "Federal securities law obligates the disclosure of *any* material network breach, including breaches involving sensitive corporate information that could be used by an adversary to gain competitive advantage in the marketplace, affect corporate earnings, and potentially reduce market share," Rockefeller writes.[89]

There is also a good case for a company to undergo an independent information security audit annually, in much the same way it gets a financial audit today. Under the Sarbanes-Oxley Act of 2002, a company's CEO and CFO have to certify that they have personally reviewed any financial reports, and that the reports are accurate.[90] A similar statement about network integrity from the CEO and the Chief Information Officer would put their personal reputations on the line—increasing management pressure to get cybersecurity right.

A third notion is to build upon the dozens of state laws that oblige firms to notify their customers when personal data—birthdates, social security numbers, bank account information and the like—have been compromised. As a tool for combating identity theft, these laws have shown some success. Sasha Romanosky and his colleagues at Carnegie Mellon University found that, between 2002 and 2009, the notification laws reduced identity theft caused by data breaches by an average of 6.1 percent.[91]

The White House recently suggested stitching the "patchwork" of 47 state data breach laws into a single—and expanded—federal one. Under the proposal, a company has 10 days to notify the federal government about security lapses that could lead to the loss of 5,000 or more customers' private information. The firm has 60 days to tell individuals about these lapses (unless the firm passes an independent security audit which deems the risk of actual data disclosure to be low). If the company complies with the new provision, it is given safe harbor from any harm that comes out of the security flaws.[92]

By targeting the breaches that expose personal information rather than the data leaks themselves, the White House's proposal could become a new corporate requirement to disclose all sorts of network security shortcomings. That would certainly benefit consumers, who might be very curious to learn which bank, utility or airline best secures its network. The bad publicity surrounding the security lapses could cause companies to shore up their networks, but as a tool for catching online criminals earlier, the administration's plan may not be quite right.

---

[89] Sen. John D. Rockefeller IV, letter to Securities and Exchange Commission Chairwoman Mary Schapiro, 5/11/2011, <http://commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e>.

[90] Morrison, Foerster, " SEC Requires CEO and CFO Certification of Quarterly and Annual Reports," 9/4/2002, <http://www.mofo.com/news/updates/files/update809.html>.

[91] Sasha Romanosky, Rahul Telang, and Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?," *Journal of Policy Analysis and Management*, 2011, <http://opimweb.wharton.upenn.edu/documents/seminars/disclosure_law_final.pdf>.

[92] Office of Management and Budget, "Complete cybersecurity proposal," 5/12/2011 <http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf>.

Under the White House proposals (and the current data breach rules), the information disclosed is *internal*: which customers had their social security numbers stolen or their banking passwords disclosed. On the other hand, many of the important indicators of a cybercriminal attack are *external*: the domain names and IP addresses used by the crooks, the tools employed to break in. If an expanded disclosure law focused on this external information, it might prove to be a better crime-fighting tool—and companies might be more willing to go along.

Taking care of your own network is, of course, the information security specialist's first and foremost job, but hardening defenses alone is not going to keep cybercriminals at bay. Sooner or later, you have to share what you know. Which makes disclosing these network breaches—in some fashion—part of the definition of 21st century corporate responsibility.

Can Insurance Curb Crime?

Today's personal data notification laws are pushing more and more companies to purchase some kind of insurance to hedge against the potential cost of a big data breach. Cybersecurity insurance policies—all but unheard-of a few years ago—have grown from a $100 million market in 2002 to an estimated $600 million in 2010.[93]

It is a positive development, writes Larry Clinton from the Internet Security Alliance: insurers "require a level of security as a precondition of coverage, and companies [that] adop[t] better security practices often receive lower insurance rates. This helps companies to internalize both the benefits of good security and the costs of poor security, which in turn leads to greater investment and improvements in cybersecurity."[94] Expanding the notification laws to include other kinds of network breaches could accelerate the market's growth even further.

RECOMMENDATION 10: REQUIRE GOVERNMENT CONTRACTORS TO CARRY CYBERSECURITY INSURANCE.
It builds the market for insurance, which encourages companies to get more serious about network protection.

Another accelerant could come from the federal government, Clinton writes. Washington could require its contractors to have cybersecurity insurance coverage. After all, the Federal Acquisition Regulations already require companies that want to do business with the government to have "insurance for certain types of perils."

The effects of insurance should not be overstated —health insurance hasn't exactly encouraged individuals to make better medical decisions, for example. But the combination of insurance and forced disclosure of network breaches should begin to give businesses some of the financial incentives needed to take greater responsibility for what happens on their networks. Both tactics should be pursued.

---

[93] Hemantha S.B. Herath and Tejaswini C. Herath, "Copula-based actuarial model for pricing cyber-insurance policies," *Insurance Markets and Companies: Analyses and Actuarial Computations*, Volume 2, Issue 1, 2011, <http://www.businessperspectives.org/journals_free/imc/2011/IMC_2011_1_Herath.pdf>.
[94] Clinton.

Criminal Enterprises, Civil Strategies

The federal government will have to use more than its purchasing power, of course, in the fight against cybercrime. It is going to need more—and better trained—law enforcement professionals.

RECOMMENDATION 11: EXPAND AND IMPROVE TRAINING FOR CYBERCRIME SPECIALISTS IN LAW ENFORCEMENT.
"The FBI is underinvesting in cyberthreats right now in the same way that it underinvested in counterterrorism in the 1990s."[95]

Of the 440 attorneys in the Justice Department's Criminal Division, for example, only 40 attorneys are specifically tasked with handling computer crimes—less than half of the number devoted to organized crime. And those lawyers are also assigned to handle intellectual property violations. As Criminal Division chief Jason Weinstein recently told Congress, "It is really undeniable that the scope of the problem, which is growing every day, far outpaces the resources that are available to pursue it currently."[96] No government manager is ever going to say he has enough resources. But in this case, the complaint seems justified.

Even more glaring are the gaps in the FBI's cyber division. Ever since bank robbers began crossing state lines in automobiles, the Bureau has been at the forefront of pursuing technology-enabled crooks. Today, the Bureau says it has "more than 1,000 advanced cyber-trained FBI agents, analysts and forensic examiners" in its 56 field offices, but those specialists are spread thin, according to an audit from the Department of Justice Inspector General, and may be misallocated.

In fiscal year 2009, the audit says, the FBI only used 31 percent of its "cyber agents" to "address criminal-based intrusions." Forty-one percent worked on "online child pornography matters," and the remainder pursued "national security intrusion investigations," intellectual property disputes, and "Internet fraud."[97] Child pornography is vile, of course, and worthy of the FBI's resources, but

---

[95] Noah Shachtman, "Inside the FBI's 'Threat Matrix,' From Nuclear Urinals to Osama's USBs," Danger Room, 5/13/2011, <http://www.wired.com/dangerroom/2011/05/inside-fbis-threat-matrix/all/1>.

[96] Andrew Ramonas, " DOJ: Computer-Based Crimes Growing; Resources Aren't," *Main Justice*, 4/12/2011, <http://www.mainjustice.com/2011/04/12/doj-computer-based-crimes-growing-resources-arent/>.

[97] U.S. Department of Justice Office of the Inspector General Audit Division, "The Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat (Redacted Version)," Audit Report 11-22, April 2011, <http://www.justice.gov/oig/reports/FBI/a1122r.pdf>.

does it deserve more attention than the countless billions being lost to online thieves and scam artists? More attention than the online attempts to compromise national security?

There is also a question about whether agents are properly trained. Auditors interviewed 36 cyber agents in 10 field offices devoted to national security investigators. More than a third said they did not have the training or expertise needed for the job. As National Security Historian Garrett Graff observes, "The FBI is underinvesting in cyberthreats right now in the same way that it underinvested in counterterrorism in the 1990s."[98]

RECOMMENDATION 12: PURSUE CIVIL STRATEGIES TO DISRUPT CRIMINAL NETWORKS.
The crooks move fast – and are often beyond American jurisdiction. Civil courts may be the only way to fracture their support system.

Piracy grew from a local nuisance to a genuine threat in distant parts of the world that seemed immune to traditional law enforcement.[99] Today, the cybercrime situation feels much the same. Online scammers and thieves are so fast-moving, so hard to find and, in many cases, so far beyond American jurisdiction, that assembling traditional criminal cases often will not work. Even when spectacular arrests are made—like the bust of credit card fraudster and online crime lord Max Butler—they seem to do little to slow the expansion of the larger cybercrime ecosystem.[100]

Some of this can be fixed by tweaking some of the relevant laws. For example, the White House recently suggested an expansion of the racketeering law to include computer crimes.[101]

In the meantime, law enforcement is turning more and more to the civil courts to disrupt the network of businesses upon which the online crook relies. In April, for instance, the Justice Department took an unprecedented step for U.S. law enforcement. It asked a judge for permission to seize the command-and-control servers of the Coreflood botnet, which is blamed for more than a million dollars in wire fraud. The judge approved the request, and the Justice Department transferred control of Coreflood to the non-profit Internet Systems Consortium.[102] The ISC began issuing "stop commands" to the millions of computers running Coreflood's malicious software, while the Justice Department e-mailed civil summonses to the "John Does" who previously ran the botnet.

Such takeovers have happened at least twice before.[103] Dutch authorities seized the servers of the Bredloab botnet in October of 2010, redirecting infected machines to a web page with instructions on how to remove the malicious software.[104] In March 2011, a federal court gave Microsoft permission to take over the Rustock botnet.[105]

The early results of the first U.S. government takeover of a botnet are promising. The number of "pings" from infected machines in the United

---

[98] Noah Shachtman, "Inside the FBI's 'Threat Matrix,' From Nuclear Urinals to Osama's USBs," Danger Room, 5/13/2011, <http://www.wired.com/dangerroom/2011/05/inside-fbis-threat-matrix/all/1>.
[99] Puchala, pg. 5.
[100] Kevin Poulsen, Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground (Crown, New York City, 2011).
[101] Office of Management and Budget, "Complete cybersecurity proposal."
[102] Kim Zetter, "With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal," Threat Level, 4/13/2011, <http://www.wired.com/threatlevel/2011/04/coreflood/>.
[103] Brian Krebs, "U.S. Government Takes Down Coreflood Botnet," *KrebsOnSecurity*, 4/14/2011, <http://krebsonsecurity.com/2011/04/u-s-government-takes-down-coreflood-botnet/>.
[104] Jeremy Kirk, "Dutch team up with Armenia for Bredolab botnet take down," *Computerworld*, 10/26/10, <https://www.computerworld.com/s/article/9193080/Dutch_team_up_with_Armenia_for_Bredolab_botnet_take_down>.
[105] Brian Krebs, "Homegrown: Rustock Botnet Fed by U.S. Firms,"*KrebsOnSecurity,* 3/21/2011, <http://krebsonsecurity.com/2011/03/homegrown-rustock-botnet-fed-by-u-s-firms/>.

States dropped by 90 percent in two weeks.[106] Unfortunately, this step does not necessarily mean the machines are disinfected—the Coreflood malware reconstitutes itself every time a machine restarts. So the FBI is now taking the additional step of deleting the program from afar, and that is potentially problematic.

Users have to provide written consent for the "uninstall," alleviating some of the civil liberties concerns that would ordinarily surround a government agency monkeying with thousands and thousands of citizens' computers. Privacy rights groups and security researchers are still worried that the untested commands could have unexpected consequences and "blow up" someone's computer.[107] As one security specialist noted, malware can be engineered to erase a machine's hard drive as soon as it is given a "stop" or "uninstall" command.[108]

Even if the Coreflood hijacking goes off without a hitch, there are legitimate long-term policy concerns if such takeovers become a regular law enforcement tool. No one would argue that innovative methods are required to smash criminally-controlled networks that can reconstitute themselves in a flash. (Rustock, for example, survived previous takedown attempts.) You do not need to be a civil liberties absolutist, however, to be uncomfortable with the idea of the government issuing commands to a citizen's computer and changing the applications inside. Law enforcement absolutely needs innovative tactics to go after an innovative underground, but it also needs to avoid the temptation to go after crooks by setting up shop inside the rest of our machines.

---

[106] Kim Zetter, "FBI vs. Coreflood Botnet: Round 1 Goes to the Feds," *Threat Level*, 4/26/2011, <http://www.wired.com/threatlevel/2011/04/coreflood_results/>.
[107] Zetter, "With Court Order..."
[108] Greg Keizer, "Feds to remotely uninstall Coreflood bot from some PCs," *Computerworld*, 4/27/2011, <https://www.computerworld.com/s/article/9216199/Feds_to_remotely_uninstall_Coreflood_bot_from_some_PCs>.

Domain Demands

The Internet is designed for anonymous and easy speech. You do not have to give your real name or your address or a social security number to register a domain name for your website. In some cases, you do not even need to pay. Getting a company to host your website on one of its machines might be slightly more expensive, but it requires no additional disclosure.

That is a very good thing for democracy advocates in the Middle East, dissidents in China and whistleblowers here at home. It also makes online crime very, very easy—"the seed from which all criminality grows," in the words of one veteran law enforcement professional.[109] Phishers, botnet herders and other crooks register all sorts of innocuous-sounding domains as fronts for their felonious activities. Then they fool otherwise-legitimate hosting companies into giving them server space for their bogus online banks and programs that give orders to botnet slaves.

Take Coreflood, the massive botnet taken down by the FBI in April. Coreflood's kingpins embedded in their malicious code a series of 25 seemingly-benign domain names—vaccina.medinnovation.org and flu.medicalcarenews.org, and the like. All the domains were registered with reputable firms, under what are believed to be pseudononymous e-mail addresses. Once the Coreflooders hijacked a computer, their newly-embedded malware ordered that machine to make contact with one of the domains and receive orders. These domains would, in turn, point back to one of two Internet Protocol addresses—servers belonging to established Dallas-based hosting companies. The whereabouts and the identities of the people behind the bot: unknown.

If anything, Coreflood used a relatively straightforward command-and-control system. It switched domains only once a month, and those domains were embedded into the malware's code. The so-called "Conficker C" malware generated 50,000 domains a *day*, seemingly at random.[110] Coreflood's domains only pointed to two IP addresses. Domains belonging to so-called "fast flux" botnets like Storm can change IP addresses every few minutes.[111]

---

[109] Private interview 4/19/11

[110] Mark Bowden, "The Enemy Within," *The Atlantic*, June, 2010, <http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/>.

[111] Dancho Danchev, "Storm Worm's Fast Flux Networks," *Dancho Danchev's Blog*, 9/5/2007, <http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html>.

Compounding the problem is that many of the registrars now give domains away—a lost leader, to attract hosting business. Crooks then pay for the server space with a stolen credit card. By the time the hosting company realizes the card is stolen—usually, it takes 30 days for payments to process—the crook is gone.

The FBI and other law enforcement agencies outlined their solution to many of these issues in a proposal to the Internet Corporation for Assigned Names and Numbers, the nonprofit company which oversees registrars and manages IP addresses. The Bureau's proposal asks, in essence, for the layer of anonymity to be stripped away from the registration and hosting industries.

The FBI plan calls for registration companies to provide authentic contact information. The registrars, in turn, should be obliged to collect—and validate—their customers' real names, e-mail addresses and credit card numbers. The customers can use proxy services to mask their identities, but the proxies would be required to collect that information as well. The proxies would then have to publish the information, if the customer is found to be violating the registrar's "terms of service, including but not limited to false data, fraudulent use, spamming and/or criminal activity."[112] Additionally, if law enforcement agencies suspect that the domain may be used for illicit activity, the authorities can use a search warrant to compel the proxies to hand over their customer information.

In some ways, it is an attractive proposition. You cannot open a physical storefront without supplying a name and address; why should a virtual storefront be any different, especially if that storefront is a criminal enterprise?

RECOMMENDATION 13: AVOID SCHEMES TO STRIP AWAY INTERNET ANONYMITY; CONTINUE TO PROMOTE FREEDOM OF ONLINE EXPRESSION.
Corralling cybercrime does not mean curbing our ideals.

The problem is that the FBI's proposal may have serious Constitutional issues. The 1st Amendment guarantees the right to free speech—and court after court has concluded that this includes a right to speak anonymously.[113] (After all, some of the Founding Fathers used pseudonyms when they wrote the Federalist Papers.)

That right cannot be used as a cover to commit crimes.[114] Under the FBI's plan, however, an online publisher could be unmasked with a warrant. That warrant can be obtained with merely a reasonable suspicion of criminal activity. The anonymity could even be stripped by a simple accusation that he did not comply with a registrar's terms of service. It is hard to see how a proposal to make anonymity that fragile squares with a right to speak without revealing your name.

It is also hard to see how the FBI proposal squares with American foreign policy. Access to the Internet—and to tools that allow anonymous speech on the Internet—have become a central pillar in the U.S. agenda. Secretary of State Clinton has called for "a global commitment to Internet freedom, to protect human rights online as we do offline."[115]

---

[112] ICANN Board, GAC Consultation: Law Enforcement Due Dilligence Recommendation – Due Dilligence and Registrar Accreditation Agreement (Draft), 2/21/2011, <http://www.icann.org/en/topics/new-gtlds/gac-board-law-enforcement-due-diligence-recommendations-21feb11-en.pdf>.

[113] Groklaw, "The First Amendment Right to Anonymous Speech - DE Ruling as Text," 10/15/2005, <http://www.groklaw.net/articlebasic.php?story=20051007151046741>.

[114] Larry Seltzer, "Anonymity Is a Problem and an American Tradition," *eWeek*, 12/21/2008, <http://www.eweek.com/c/a/Security/Anonymity-is-a-Problem-and-an-American-Tradition/1/>.

[115] Hillary Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World," 2/25/2011, <http://www.state.gov/secretary/rm/2011/02/156619.htm>.

President Obama echoed that sentiment, saying, "There are certain core values that … we believe are universal: freedom of speech, freedom of expression, people being able to use social networking."[116] Long before Obama took office, America had already spent tens of millions of dollars building and distributing tools for anonymous online speech. Tor, the software developed by the U.S. Navy to route Internet traffic through a series of encrypted nodes, is one example of many.[117]

Yet the ongoing abuse of the registration and hosting systems could well undermine all other efforts to fight cybercrime. This demands some sort of change to prevent that abuse. If crooks are using stolen credit cards to buy up domains and server space, perhaps customers paying with credit cards should be forced to wait 30 days until the transactions have been processed. (Domains could still be reserved instantly, and cash-equivalent payments would allow the consumer to start using the services right away.)

Brookings Fellow Allan Friedman suggests that, at the very least, the costs of abusing the registration and hosting systems should be raised. Friedman's concept requires customers to pay a bond, or temporary deposit, on top of any fees. "This would raise the cost of registering many domains, but impose little long run cost on a legitimate user. Bad actors could still acquire domains and hold them long enough for the refunded bond, but it would still impose a larger up front investment cost," he writes. "It would also expose the malicious actor to the risk of forfeiture, should the domains be recognized as potentially malicious during the bond period."[118]

In other words, the Conficker tactic of registering tens of thousands of domains would suddenly get much, much more expensive, while legitimate users would get their deposit back after some period of time—say six months or a year.

Would this slow down the most serious criminal enterprises? Not a chance; they already spend the money to set up their own registration firms. A few extra dollars per domain is just a rounding error, but even if it simply imposes a small tax on online crooks, the proposal has merit—as one piece in a larger effort designed to push cybercriminals to the margins.

---

[116] Spencer Ackerman, "Egypt's Internet Shutdown Can't Stop Mass Protests," *Danger Room*, 1/28/2011, <http://www.wired.com/dangerroom/2011/01/egypts-internet-shutdown-cant-stop-mass-protests/>.

[117] Eli Lake, "Iranian protesters avoid censorship with Navy technology," Washington Times, 6/26/09, <http://www.washingtontimes.com/news/2009/jun/26/protesters-use-navy-technology-to-avoid-censorship/>.

[118] Allan Friedman, "Anonymity Bonds," unpublished, 2011.

Thirteen Steps

Online crime may seem to be an unsolvable problem—the consequence of an Internet in which anonymity is hardwired and jurisdictions are meaningless—but there are steps that can be taken to curb the growth of cybercrime and marginalize the people who practice it.

Furthermore, more, there is a growing sense among the world's leading countries that the rampant spread of online crime has to be met head on. The countries accused of being the biggest homes to cybercriminals—notably the United States and China—are the ones who feel most victimized. There is an opportunity for dialogue and cooperation on cybercrime—dialogue and cooperation that could build understanding on strategic issues as well.

In the end, however, it is companies, not governments, that will have to play the central role in the fight against cybercrime. Internet Service Providers, which control access to the broader of network of networks, will be particularly essential.

It is no secret which companies most consistently provide server space and other support services to online criminals. The trick is persuading ISPs to throttle or block that criminal-friendly traffic. If this relatively small group of ISPs can be persuaded to move against online criminals—and the companies that support them—it will be an enormous step towards turning these crooks into global pariahs.

One method is to hold the most criminally-connected hosting companies liable for any harm that may arise from activities on its servers, and hold ISPs liable if they continue to do business with that hosting firm.

This would be part of a broader push to elbow out cybercriminals, while preserving the Internet's essential, freewheeling nature—and maintaining the American ideals of free speech. Our recommendations are:

1. Begin U.S.-China talks focused on cybercrime.
2. Draw China into the larger community of ISPs and network carriers.
3. Avoid national retaliation as a cybercrime solution.
4. Lean on the criminal support networks.
5. Motivate ISPs to pressure the criminal ecosystem.
6. Hold the worst hosting companies liable for their criminal clients and the worst ISPs liable for their criminal hosts.

7. Encourage ISPs to notify customers of infections.
8. Amend the laws to allow ISPs to share attack data.
9. Push companies to expand reporting of network breaches.
10. Require government contractors to have cybersecurity insurance.
11. Expand and improve training for cybercrime specialists in law enforcement.
12. Pursue civil strategies to disrupt criminal networks.
13. Avoid schemes to strip away Internet anonymity; continue to promote freedom of online expression.

These steps will not eliminate cybercrime any more than the early moves to shut down the pirate support networks brought an end to the hijacking. They do not have to. The Internet community has shown a remarkable ability to continue expanding, year after year, despite seemingly gargantuan obstacles at every turn. Spam was supposed to wipe out email; lack of bandwidth was supposed to slow web sites to a crawl; the dot-com crash was supposed to wipe out the Internet's innovative spirit; flaws in the DNS system were supposed to result in a doomsday attack. At every turn, those challenges were eventually met and surpassed. The same could very well be true of online crime. If the the rise of these criminal enterprises can merely be slowed down, the Internet, in all its resilience, may take care of the rest.

About the Author

NOAH SHACHTMAN is a nonresident fellow inthe Brookings Institution's 21st Century Defense Initiative. He is also a contributing editor at *Wired* magazine and editor of the national security blog *Danger Room*. Shachtman has reported from Afghanistan, Israel, Iraq, the Pentagon and Los Alamos, writing about technology and national security for *The Wall Street Journal*, *The New York Times Magazine*, *Foreign Policy*, and *The Bulletin of the Atomic Scientists*, among others. The Offices of the Undersecretary of Defense for Intelligence, the Undersecretary of Defense for Policy, and the Director of National Intelligence have all asked him to contribute to discussions on cybersecurity, information operations and emerging threats. Shachtman lives in Brooklyn, New York with his wife, Elizabeth, and their son, Leo.

BROOKINGS
1775 Massachusetts Ave., NW
Washington, D.C. 20036
brookings.edu