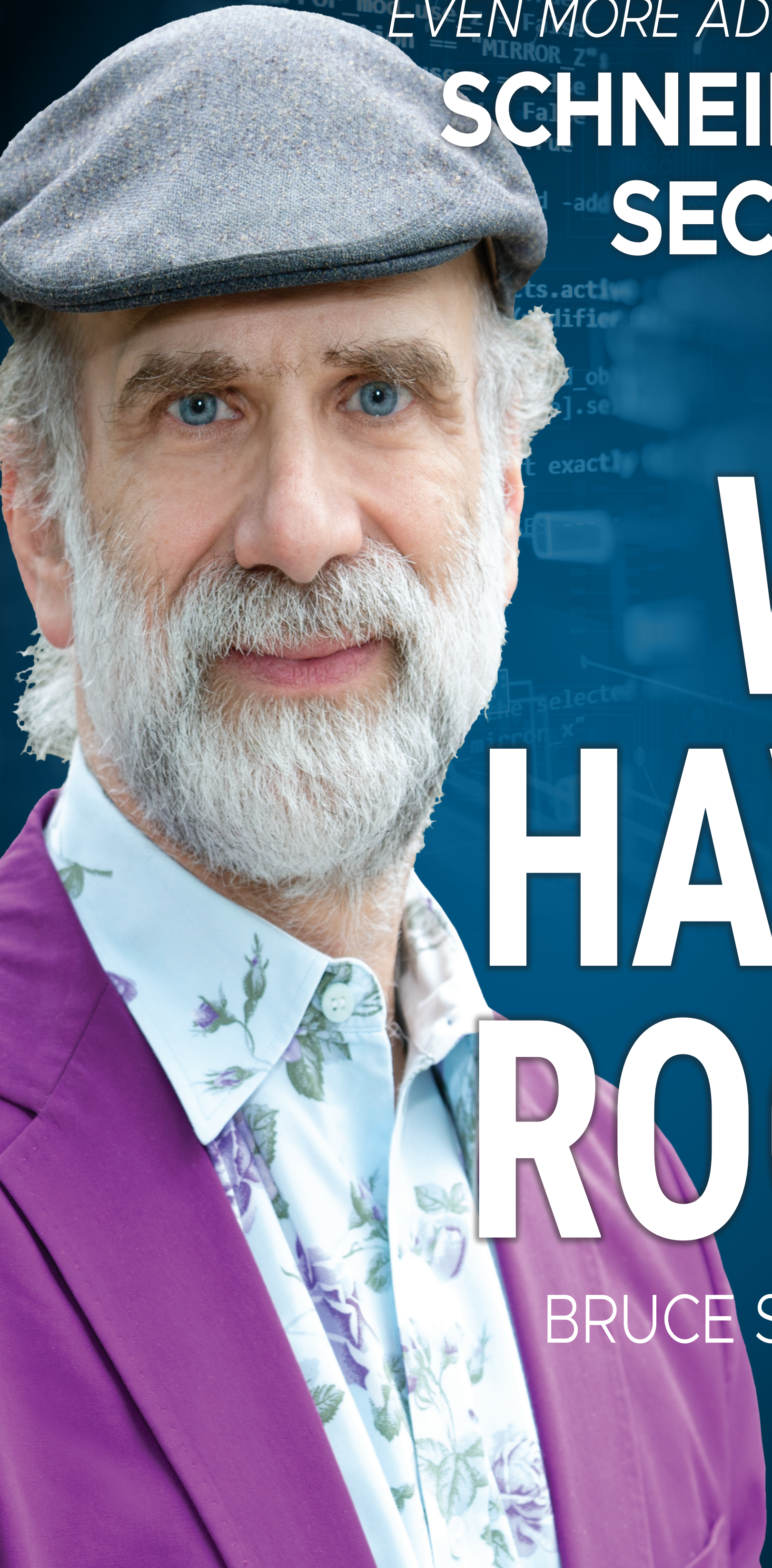
EVEN MORE ADVICE FROM

SCHNEIER ON SECURITY

WE HAVE ROOT

BRUCE SCHNEIER



WILEY

We Have Root

We Have Root

Even More Advice from Schneier on Security

Bruce Schneier

WILEY

We Have Root: Even More Advice from Schneier on Security

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-64301-2
ISBN: 978-1-119-64346-3 (ebk)
ISBN: 978-1-119-64312-8 (ebk)

Manufactured in the United States of America

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2019945771

About the Author

Bruce Schneier is an internationally renowned security technologist, called a security guru by the *Economist*. He is the author of 14 books—including the best-seller *Click Here to Kill Everybody*—as well as hundreds of articles, essays, and academic papers. His influential newsletter Crypto-Gram and blog Schneier on Security are read by over 250,000 people. Schneier is a fellow at the Berkman Klein Center for Internet and Society at Harvard University; a Lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; and an advisory board member of EPIC and VerifiedVoting.org. He can be found online at `www.schneier.com` and `@schneierblog`.

Contents

Introduction

Why I Write about Tech for Popular Audiences

I write essays because I enjoy it. It's fun, and I'm good at it. I like the exposure. Having an essay published in a popular and influential newspaper or magazine is a good way to get new readers. And having to explain something to a general audience in 1,200 words is a good way for me to crystallize my own thinking.

That's not all: I also write because it's important.

I consider myself a technologist. Technology is complicated. It requires expertise to understand. Technological systems are full of nonlinear effects, emergent properties, and wicked problems. In the broader context of how we use technology, they are complex socio-technical systems. These socio-technical systems are also full of even-more-complex nonlinear effects, emergent properties, and wicked problems. Understanding all this is hard: it requires understanding both the underlying technology and the broader social context. Explaining any of this to a popular audience is even harder. But it's something that technologists need to do.

We need to do it because understanding it matters.

What really matters is not the technology part, but the socio-technical whole. Addressing Congress in a 2011 essay, journalist Joshua Kopstein wrote: "It's no longer OK not to understand how the Internet works." He's right, but he's also wrong. The Internet is pervasive and powerful precisely because you do not need to understand how it works. You can just use it, just as you use any other specialized hard-to-understand technology. Similarly, Congress doesn't need to understand how the Internet works in order to effectively legislate it. It had better not be true that only those who know how something works can effectively legislate. We know that governments that can legislate aviation without understanding aerodynamics, health without understanding medicine, and climate change without understanding the science of climate change.

Where Kopstein is right is that policy makers need to understand enough about how the Internet works to understand its broader socio-technical implications, and enough about how the Internet works to defer to technologists when they reach the end of their understanding—just as they need to do with aviation, health, and the enormous ongoing catastrophe that is climate change. When policy makers ignore the science and tech in favor of their own agendas, or when they defer to lobbyists, tech policy starts to go off the rails. It is our job as technologists to explain what we do to a broader audience. Not just now technology works, but how it fits in to society. We have a unique perspective.

It's also a vital perspective. Kopstein is also right when he said that "it's no longer okay." It once was okay, but now it's not. The Internet, and information technologies in general, are fundamental to society. In some ways, this is a surprise. The people who designed and built the Internet created a system that—at its start—didn't matter. Email, file transfer, remote access, webpages—even commerce—were nice-to-have add-ons. They might have been important to us, but they weren't important to society. This has completely changed. The Internet is vital to society. Social media is vital to public discourse. The web is vital for commerce. Even more critically, the Internet now affects the world in a direct physical manner. And in the future, as the Internet of Things permeates more of our society, the Internet will directly affect life and property. And, of course, enable a level of pervasive surveillance the world has never seen.

This is what policy makers, and everyone else, needs, to understand. This is what we need to help explain.

One of the ways we can help bridge this gap is by writing about technology for popular audiences. Whether it's security and privacy—my areas of expertise—artificial intelligence and robotics, algorithms, synthetic biology, food security, climate change, or any of the other major science and technology issues facing society, we technologists need to share what we know.

This is one aspect of what is coming to be known as public-interest technology. It's a broad umbrella of a term, encompassing technologists who work on public policy—either inside government or from without—people who work on technological projects for the public good, academics who teach courses at the intersection of technology and policy, and a lot more. It's what we need more of in a world where society's critical problems have a strong technological basis—and whose solutions will be similarly technological.

This is my third volume of essays, covering July 2013 through December 2017. It includes essays on topics I have written about for decades, like privacy and surveillance. It includes essays on topics that are pretty new to me, like the Internet of Things. It includes essays written during the period that Edward Snowden's NSA documents were made public. Every word in this book has been published elsewhere (including these), and all are available for free on my website. What this book does is make them available in a curated-by-topic, easy-to-carry, ink-on-paper format that I hope looks good on your shelf. Or an e-book version, if you prefer to read that way.

Over the course of my career, I've written over 600 essays and op-eds. I wouldn't do it—I couldn't do it—if you weren't reading them. Thank you for that.

1 Crime, Terrorism, Spying, and War

Cyberconflicts and National Security

Originally published in UN Chronicle, *July 18, 2013*

Whenever national cybersecurity policy is discussed, the same stories come up again and again. Whether the examples are called acts of cyberwar, cyberespionage, hacktivism, or cyberterrorism, they all affect national interest, and there is a corresponding call for some sort of national cyberdefense.

Unfortunately, it is very difficult to identify attackers and their motivations in cyberspace. As a result, nations are classifying all serious cyberattacks as cyberwar. This perturbs national policy and fuels a cyberwar arms race, resulting in more instability and less security for everyone. We need to dampen our cyberwar rhetoric, even as we adopt stronger law enforcement policies towards cybersecurity, and work to demilitarize cyberspace.

Let us consider three specific cases:

In Estonia, in 2007, during a period of political tensions between the Russian Federation and Estonia, there were a series of denial-of-service cyberattacks against many Estonian websites, including those run by the Estonian Parliament, government ministries, banks, newspapers and television stations. Though Russia was blamed for these attacks based on circumstantial evidence, the Russian Government never admitted its involvement. An ethnic Russian living in Tallinn, who was upset by Estonia's actions and who had been acting alone, was convicted in an Estonian court for his part in these attacks.

In Dharamsala, India, in 2009, security researchers uncovered a sophisticated surveillance system in the Dalai Lama's computer network. Called GhostNet, further research found the same network had infiltrated political, economic and media targets in 103 countries. China was the presumed origin of this surveillance network, although the evidence was circumstantial. It was also unclear whether this network was run by an organization of the Chinese Government, or by Chinese nationals for either profit or nationalist reasons.

In Iran, in 2010, the Stuxnet computer worm severely damaged, and possibly destroyed, centrifuge machines in the Natanz uranium enrichment facility, in an effort to set back the Iranian nuclear program. Subsequent analysis of the worm indicated that it was a well-designed and well-executed cyberweapon, requiring an engineering effort that implied a nation-state sponsor. Further investigative reporting pointed to the United States and Israel as designers and deployers of the worm, although neither country has officially taken credit for it.

Ordinarily, you could determine who the attacker was by the weaponry. When you saw a tank driving down your street, you knew the military was involved because only the military could afford tanks. Cyberspace is different. In cyberspace, technology is broadly spreading its capability, and everyone is using the same weaponry: hackers, criminals, politically motivated hacktivists, national spies, militaries, even the potential cyberterrorist. They are all exploiting the same vulnerabilities, using the same sort of hacking tools, engaging in the same attack tactics, and leaving the same traces behind. They all eavesdrop or steal data. They all engage in denial-of-service attacks. They all probe cyberdefenses and do their best to cover their tracks.

Despite this, knowing the attacker is vitally important. As members of society, we have several different types of organizations that can defend us from an attack. We can call the police or the military. We can call on our national anti-terrorist agency and our corporate lawyers. Or we can defend ourselves with a variety of commercial products and services. Depending on the situation, all of these are reasonable choices.

The legal regime in which any defense operates depends on two things: who is attacking you and why. Unfortunately, when you are being attacked in cyberspace, the two things you often do not know are who is attacking you and why. It is not that everything can be defined as cyberwar; it is that we are increasingly seeing warlike tactics used in broader cyberconflicts. This makes defense and national cyberdefense policy difficult.

The obvious tendency is to assume the worst. If every attack is potentially an act of war perpetrated by a foreign military, then the logical assumption is that the military needs to be in charge of all cyberdefense, and military problems beg for military solutions. This is the rhetoric we hear from many of the world's leaders: the problem is cyberwar and we are all fighting one right now. This is just not true; there is no war in cyberspace. There is an enormous amount of criminal activity, some of it organized and much of it international. There is politically motivated hacking—hacktivism—against countries, companies, organizations and individuals. There is espionage, sometimes by lone actors and sometimes by national espionage organizations. There are also offensive actions by national organizations, ranging from probing each other's cyberdefenses to actual damage-causing cyberweapons like Stuxnet.

The word "war" really has two definitions: the literal definition of war which evokes guns and tanks and advancing armies, and the rhetorical definition of war as in war on crime, war on poverty, war on drugs, and war on terror. The term "cyberwar" has aspects of both literal and rhetorical war, making it a very loaded term to use when discussing cybersecurity and cyberattacks.

Words matter. To the police, we are citizens to protect. To the military, we are a population to be managed. Framing cybersecurity in terms of war reinforces the notion that we are helpless in the face of the threat, and we need a government—indeed, a military—to protect us.

The framing of the issue as a war affects policy debates around the world. From the notion of government control over the Internet, to wholesale surveillance and eavesdropping facilitation, to an Internet kill switch, to calls to eliminate anonymity—many measures proposed by different countries might make sense in wartime but not in peacetime. (Except that like the war on drugs or terror, there is no winning condition, which means placing a population in a permanent state of emergency). We are seeing a power grab in cyberspace by the world's militaries. We are in the early years of a cyberwar arms race.

Arms races stem from ignorance and fear: ignorance of the other side's capabilities and fear that its capabilities are greater than one's own. Once cyberweapons exist, there will be an impetus to use them.

Stuxnet damaged networks other than its intended targets. Any military-inserted back doors in Internet systems will make us more vulnerable to criminals and hackers.

The cyberwar arms race is destabilizing. It is only a matter of time before something big happens, perhaps by the rash actions of a low-level military officer, an enthusiastic hacker who thinks he is working in his country's best interest, or by accident. If the target nation retaliates, we could find ourselves in a real cyberwar.

I am not proposing that cyberwar is complete fiction. War expands to fill all available theatres, and any future war will have a cyberspace component. It makes sense for countries to establish cyberspace commands within their militaries, and to prepare for cyberwar. Similarly, cyberespionage is not going away anytime soon. Espionage is as old as civilization, and there is simply too much good information in cyberspace for countries not to avail themselves of hacking tools to get at it.

We need to dampen the war rhetoric and increase international cybersecurity cooperation. We need to continue talking about cyberwar treaties. We need to establish rules of engagement in cyberspace, including ways to identify where attacks are coming from and clear definitions of what does or does not constitute an offensive action. We need to understand the role of cybermercenaries, and the role of non-state actors. Cyberterrorism is still a media and political myth, but there will come a time when it will not be. Lastly, we need to build resilience into our infrastructure. Many cyberattacks, regardless of origin, exploit fragilities in the Internet. The more we can reduce those, the safer we will be.

Cyberspace threats are real, but militarizing cyberspace will do more harm than good. The value of a free and open Internet is too important to sacrifice to our fears.

Counterterrorism Mission Creep

Originally published in TheAtlantic.com, *July 16, 2013*

One of the assurances I keep hearing about the US government's spying on American citizens is that it's only used in cases of terrorism. Terrorism is, of course, an extraordinary crime, and its horrific nature is supposed to justify permitting all sorts of excesses to prevent it. But there's a problem with this line of reasoning: mission creep. The definitions of "terrorism" and "weapon of mass destruction" are broadening, and these extraordinary powers are being used, and will continue to be used, for crimes other than terrorism.

Back in 2002, the Patriot Act greatly broadened the definition of terrorism to include all sorts of "normal" violent acts as well as nonviolent protests. The term "terrorist" is surprisingly broad; since the terrorist attacks of 9/11, it has been applied to people you wouldn't normally consider terrorists.

The most egregious example of this are the three anti-nuclear pacifists, including an 82-year-old nun, who cut through a chain-link fence at the Oak Ridge nuclear-weapons-production facility in 2012. While they were originally arrested on a misdemeanor trespassing charge, the government kept increasing their charges as the facility's security lapses became more embarrassing. Now the protestors have been convicted of violent crimes of terrorism—and remain in jail.

Meanwhile, a Tennessee government official claimed that complaining about water quality could be considered an act of terrorism. To the government's credit, he was subsequently demoted for those remarks.

The notion of making a terrorist threat is older than the current spate of anti-terrorism craziness. It basically means threatening people in order to terrorize them, and can include things like pointing a fake gun at someone, threatening to set off a bomb, and so on. A Texas high-school student recently spent five months in jail for writing the following on Facebook: "I think I'ma shoot up a kindergarten. And watch the blood of the innocent rain down. And eat the beating heart of one of them." Last year, two Irish tourists were denied entry at the Los Angeles Airport because of some misunderstood tweets.

Another term that's expanded in meaning is "weapon of mass destruction." The law is surprisingly broad, and includes anything that explodes, leading political scientist and terrorism-fear skeptic John Mueller to comment:

> *As I understand it, not only is a grenade a weapon of mass destruction, but so is a maliciously-designed child's rocket*

> *even if it doesn't have a warhead. On the other hand, although a missile-propelled firecracker would be considered a weapon of mass destruction if its designers had wanted to think of it as a weapon, it would not be so considered if it had previously been designed for use as a weapon and then redesigned for pyrotechnic use or if it was surplus and had been sold, loaned, or given to you (under certain circumstances) by the secretary of the army...*
>
> *All artillery, and virtually every muzzle-loading military long arm for that matter, legally qualifies as a WMD. It does make the bombardment of Ft. Sumter all the more sinister. To say nothing of the revelation that The Star Spangled Banner is in fact an account of a WMD attack on American shores.*

After the Boston Marathon bombings, one commentator described our use of the term this way: "What the United States means by terrorist violence is, in large part, 'public violence some weirdo had the gall to carry out using a weapon other than a gun.' ... Mass murderers who strike with guns (and who don't happen to be Muslim) are typically read as psychopaths disconnected from the larger political sphere." Sadly, there's a lot of truth to that.

Even as the definition of terrorism broadens, we have to ask how far we will extend that arbitrary line. Already, we're using these surveillance systems in other areas. A raft of secret court rulings has recently expanded the NSA's eavesdropping powers to include "people possibly involved in nuclear proliferation, espionage and cyberattacks." A "little-noticed provision" in a 2008 law expanded the definition of "foreign intelligence" to include "weapons of mass destruction," which, as we've just seen, is surprisingly broad.

A recent *Atlantic* essay asks, somewhat facetiously, "If PRISM is so good, why stop with terrorism?" The author's point was to discuss the value of the Fourth Amendment, even if it makes the police less efficient. But it's actually a very good question. Once the NSA's ubiquitous surveillance of all Americans is complete—once it has the ability to collect and process all of our emails, phone calls, text messages, Facebook posts, location data, physical mail, financial transactions, and who knows what else—why limit its use to cases of terrorism? I can easily imagine a public groundswell of support to use to help solve some other heinous crime, like a kidnapping.

Or maybe a child-pornography case. From there, it's an easy step to enlist NSA surveillance in the continuing war on drugs; that's certainly important enough to warrant regular access to the NSA's databases. Or maybe to identify illegal immigrants. After all, we've already invested in this system, we might as well get as much out of it as we possibly can. Then it's a short jump to the trivial examples suggested in the *Atlantic* essay: speeding and illegal downloading. This "slippery slope" argument is largely speculative, but we've already started down that incline.

Criminal defendants are starting to demand access to the NSA data that they believe will exonerate themselves. How can a moral government refuse this request?

More humorously, the NSA might have created the best backup system ever.

Technology changes slowly, but political intentions can change very quickly. In 2000, I wrote in my book *Secrets and Lies* about police surveillance technologies: "Once the technology is in place, there will always be the temptation to use it. And it is poor civic hygiene to install technologies that could someday facilitate a police state." Today we're installing technologies of ubiquitous surveillance, and the temptation to use them will be overwhelming.

Syrian Electronic Army Cyberattacks

Originally published in the Wall Street Journal website,
August 29, 2013

The Syrian Electronic Army attacked again this week, compromising the websites of the *New York Times*, Twitter, the Huffington Post, and others.

Political hacking isn't new. Hackers were breaking into systems for political reasons long before commerce and criminals discovered the Internet. Over the years, we've seen U.K. vs. Ireland, Israel vs. Arab states, Russia vs. its former Soviet republics, India vs. Pakistan, and US vs. China.

There was a big one in 2007, when the government of Estonia was attacked in cyberspace following a diplomatic incident with Russia. It was hyped as the first cyberwar, but the Kremlin denied any Russian government involvement. The only individuals positively identified were young ethnic Russians living in Estonia.

Poke at any of these international incidents, and what you find are kids playing politics. The Syrian Electronic Army doesn't seem to be an actual army. We don't even know if they're Syrian. And—to be fair—I don't know their ages. Looking at the details of their attacks, it's pretty clear they didn't target the *New York Times* and others directly. They reportedly hacked into an Australian domain name registrar called Melbourne IT, and used that access to disrupt service at a bunch of big-name sites.

We saw this same tactic last year from Anonymous: hack around at random, then retcon a political reason why the sites they successfully broke into deserved it. It makes them look a lot more skilled than they actually are.

This isn't to say that cyberattacks by governments aren't an issue, or that cyberwar is something to be ignored. Attacks from China reportedly are a mix of government-executed military attacks, government-sponsored independent attackers, and random hacking groups that work with tacit government approval. The US also engages in active cyberattacks around the world. Together with Israel, the US employed a sophisticated computer virus (Stuxnet) to attack Iran in 2010.

For the typical company, defending against these attacks doesn't require anything different than what you've been traditionally been doing to secure yourself in cyberspace. If your network is secure, you're secure against amateur geopoliticians who just want to help their side.

The Limitations of Intelligence

Originally published in CNN.com, *September 11, 2013*

We recently learned that US intelligence agencies had at least three days' warning that Syrian President Bashar al-Assad was preparing to launch a chemical attack on his own people, but wasn't able to stop it. At least that's what an intelligence briefing from the White House reveals. With the combined abilities of our national intelligence apparatus—the CIA, NSA, National Reconnaissance Office and all the rest—it's not surprising that we had advance notice. It's not known whether the US shared what it knew.

More interestingly, the US government did not choose to act on that knowledge (for example, launch a preemptive strike), which left some wondering why.

There are several possible explanations, all of which point to a fundamental problem with intelligence information and our national intelligence apparatuses.

The first possibility is that we may have had the data, but didn't fully understand what it meant. This is the proverbial connect-the-dots problem. As we've learned again and again, connecting the dots is hard. Our intelligence services collect billions of individual pieces of data every day. After the fact, it's easy to walk backward through the data and notice all the individual pieces that point to what actually happened. Before the fact, though, it's much more difficult. The overwhelming majority of those bits of data point in random directions, or nowhere at all. Almost all the dots don't connect to anything.

Rather than thinking of intelligence as a connect-the-dots picture, think of it as a million unnumbered pictures superimposed on top of each other. Which picture is the relevant one? We have no idea. Turning that data into actual information is an extraordinarily difficult problem, and one that the vast scope of our data-gathering programs makes even more difficult.

The second possible explanation is that while we had some information about al-Assad's plans, we didn't have enough confirmation to act on that information. This is probably the most likely explanation. We can't act on inklings, hunches, or possibilities. We probably can't even act on probabilities; we have to be sure. But when it comes to intelligence, it's hard to be sure. There could always be something else going on—something we're not able to eavesdrop on, spy on, or see from our satellites. Again, our knowledge is most obvious after the fact.

The third is that while we were sure of our information, we couldn't act because that would reveal "sources and methods." This is probably the most frustrating explanation. Imagine we are able to eavesdrop on al-Assad's most private conversations with his generals and aides, and are absolutely sure of his plans. If we act on them, we reveal that we are eavesdropping. As a result, he's likely to change how he communicates, costing us our ability to eavesdrop. It might sound perverse, but often the fact that we are able to successfully spy on someone is a bigger secret than the information we learn from that spying.

This dynamic was vitally important during World War II. During the war, the British were able to break the German Enigma encryption machine and eavesdrop on German military communications. But while the Allies knew a lot, they would only act on information they learned when there was another plausible way they could have learned it. They even occasionally manufactured plausible explanations. It was just too risky to tip the Germans off that their encryption machines' code had been broken.

The fourth possibility is that there was nothing useful we could have done. And it is hard to imagine how we could have prevented the use of chemical weapons in Syria. We couldn't have launched a preemptive strike, and it's probable that it wouldn't have been effective. The only feasible action would be to alert the opposition—and that, too, might not have accomplished anything. Or perhaps there wasn't sufficient agreement for any one course of action—so, by default, nothing was done.

All of these explanations point out the limitations of intelligence. The NSA serves as an example. The agency measures its success by amount of data collected, not by information synthesized or knowledge gained. But it's knowledge that matters.

The NSA's belief that more data is always good, and that it's worth doing anything in order to collect it, is wrong. There are diminishing returns, and the NSA almost certainly passed that point long ago. But the idea of trade-offs does not seem to be part of its thinking.

The NSA missed the Boston Marathon bombers, even though the suspects left a really sloppy Internet trail and the older brother was on the terrorist watch list. With all the NSA is doing eavesdropping on the world, you would think the least it could manage would be keeping track of people on the terrorist watch list. Apparently not.

I don't know how the CIA measures its success, but it failed to predict the end of the Cold War.

More data does not necessarily mean better information. It's much easier to look backward than to predict. Information does not necessarily enable the government to act. Even when we know something, protecting the methods of collection can be more valuable than the possibility of taking action based on gathered information. But there's not a lot of value to intelligence that can't be used for action. These are the paradoxes of intelligence, and it's time we started remembering them.

Of course, we need organizations like the CIA, the NSA, the NRO and all the rest. Intelligence is a vital component of national security, and can be invaluable in both wartime and peacetime. But it is just one security tool among many, and there are significant costs and limitations.

We've just learned from the recently leaked "black budget" that we're spending $52 billion annually on national intelligence. We need to take a serious look at what kind of value we're getting for our money, and whether it's worth it.

Computer Network Exploitation vs. Computer Network Attack

Originally published in TheAtlantic.com, *March 6, 2014*

Back when we first started getting reports of the Chinese breaking into US computer networks for espionage purposes, we described it in some very strong language. We called the Chinese actions cyber-attacks. We sometimes even invoked the word cyberwar, and declared that a cyber-attack was an act of war.

When Edward Snowden revealed that the NSA has been doing exactly the same thing as the Chinese to computer networks around the world, we used much more moderate language to describe US actions: words like espionage, or intelligence gathering, or spying. We stressed that it's a peacetime activity, and that everyone does it.

The reality is somewhere in the middle, and the problem is that our intuitions are based on history.

Electronic espionage is different today than it was in the pre-Internet days of the Cold War. Eavesdropping isn't passive anymore. It's not the electronic equivalent of sitting close to someone and overhearing a conversation. It's not passively monitoring a communications circuit. It's more likely to involve actively breaking into an adversary's computer network—be it Chinese, Brazilian, or Belgian—and installing malicious software designed to take over that network.

In other words, it's hacking. Cyber-espionage is a form of cyber-attack. It's an offensive action. It violates the sovereignty of another country, and we're doing it with far too little consideration of its diplomatic and geopolitical costs.

The abbreviation-happy US military has two related terms for what it does in cyberspace. CNE stands for "computer network exploitation."

That's spying. CNA stands for "computer network attack." That includes actions designed to destroy or otherwise incapacitate enemy networks. That's—among other things—sabotage.

CNE and CNA are not solely in the purview of the US; everyone does it. We know that other countries are building their offensive cyberwar capabilities. We have discovered sophisticated surveillance networks from other countries with names like GhostNet, Red October, The Mask. We don't know who was behind them—these networks are very difficult to trace back to their source—but we suspect China, Russia, and Spain, respectively. We recently learned of a hacking tool called RCS that's used by 21 governments: Azerbaijan, Colombia, Egypt, Ethiopia, Hungary, Italy, Kazakhstan, Korea, Malaysia, Mexico, Morocco, Nigeria, Oman, Panama, Poland, Saudi Arabia, Sudan, Thailand, Turkey, UAE, and Uzbekistan.

When the Chinese company Huawei tried to sell networking equipment to the US, the government considered that equipment a "national security threat," rightly fearing that those switches were backdoored to allow the Chinese government both to eavesdrop and attack US networks. Now we know that the NSA is doing the exact same thing to American-made equipment sold in China, as well as to those very same Huawei switches.

The problem is that, from the point of view of the object of an attack, CNE and CNA look the same as each other, except for the end result. Today's surveillance systems involve breaking into the computers and installing malware, just as cybercriminals do when they want your money. And just like Stuxnet: the US/Israeli cyberweapon that disabled the Natanz nuclear facility in Iran in 2010.

This is what Microsoft's General Counsel Brad Smith meant when he said: "Indeed, government snooping potentially now constitutes an 'advanced persistent threat,' alongside sophisticated malware and cyber attacks."

When the Chinese penetrate US computer networks, which they do with alarming regularity, we don't really know what they're doing. Are they modifying our hardware and software to just eavesdrop, or are they leaving "logic bombs" that could be triggered to do real damage at some future time? It can be impossible to tell. As a 2011 EU cybersecurity policy document stated (page 7):

> *...technically speaking, CNA requires CNE to be effective. In other words, what may be preparations for cyberwarfare can well be cyberespionage initially or simply be disguised as such.*

We can't tell the intentions of the Chinese, and they can't tell ours, either.

Much of the current debate in the US is over what the NSA should be allowed to do, and whether limiting the NSA somehow empowers other governments. That's the wrong debate. We don't get to choose between a world where the NSA spies and one where the Chinese spy. Our choice is between a world where our information infrastructure is vulnerable to all attackers or secure for all users.

As long as cyber-espionage equals cyber-attack, we would be much safer if we focused the NSA's efforts on securing the Internet from these attacks. True, we wouldn't get the same level of access to information flows around the world. But we would be protecting the world's information flows—including our own—from both eavesdropping and more damaging attacks. We would be protecting our information flows from governments, nonstate actors, and criminals. We would be making the world safer.

Offensive military operations in cyberspace, be they CNE or CNA, should be the purview of the military. In the US, that's CyberCommand. Such operations should be recognized as offensive military actions, and should be approved at the highest levels of the executive branch, and be subject to the same international law standards that govern acts of war in the offline world.

If we're going to attack another country's electronic infrastructure, we should treat it like any other attack on a foreign country. It's no longer just espionage, it's a cyber-attack.

iPhone Encryption and the Return of the Crypto Wars

Originally published in CNN.com, *October 3, 2014*

Last week, Apple announced that it is closing a serious security vulnerability in the iPhone. It used to be that the phone's encryption only protected a small amount of the data, and Apple had the ability to bypass security on the rest of it.

From now on, all the phone's data is protected. It can no longer be accessed by criminals, governments, or rogue employees. Access to it can no longer be demanded by totalitarian governments. A user's iPhone data is now more secure.

To hear US law enforcement respond, you'd think Apple's move heralded an unstoppable crime wave. See, the FBI had been using that vulnerability to get into people's iPhones. In the words of cyberlaw professor Orin Kerr, "How is the public interest served by a policy that only thwarts lawful search warrants?"

Ah, but that's the thing: You can't build a backdoor that only the good guys can walk through. Encryption protects against cybercriminals, industrial competitors, the Chinese secret police and the FBI. You're either vulnerable to eavesdropping by any of them, or you're secure from eavesdropping from all of them.

Backdoor access built for the good guys is routinely used by the bad guys. In 2005, some unknown group surreptitiously used the lawful-intercept capabilities built into the Greek cell phone system. The same thing happened in Italy in 2006.

In 2010, Chinese hackers subverted an intercept system Google had put into Gmail to comply with US government surveillance requests. Back doors in our cell phone system are currently being exploited by the FBI and unknown others.

This doesn't stop the FBI and Justice Department from pumping up the fear. Attorney General Eric Holder threatened us with kidnappers and sexual predators.

The former head of the FBI's criminal investigative division went even further, conjuring up kidnappers who are also sexual predators. And, of course, terrorists.

FBI Director James Comey claimed that Apple's move allows people to "place themselves beyond the law" and also invoked that now overworked "child kidnapper." John J. Escalante, chief of detectives for the Chicago police department now holds the title of most hysterical: "Apple will become the phone of choice for the pedophile."

It's all bluster. Of the 3,576 major offenses for which warrants were granted for communications interception in 2013, exactly one involved kidnapping. And, more importantly, there's no evidence that encryption hampers criminal investigations in any serious way. In 2013, encryption foiled the police nine times, up from four in 2012—and the investigations proceeded in some other way.

This is why the FBI's scare stories tend to wither after public scrutiny. A former FBI assistant director wrote about a kidnapped man who would never have been found without the ability of the FBI to