

CHAPTER 2

System Crash

If we continue to develop our technology without wisdom or prudence, our servant may prove to be our executioner.
OMAR N. BRADLEY

Something had to be wrong with the signals. It was a Tuesday in early January 2008 when a tram in Lodz, Poland, suddenly veered to the left. This in itself wasn't so strange—except for the fact that the conductor had been attempting to turn his train right. Moments later, the rear cars skidded off the rails before crashing into another tram and coming to a screeching halt.

Amazingly, given the size of the collision, no one was killed, but more than a dozen passengers were injured, and many others were left scratching their heads. What had gone wrong? Rather than a circuit failure or human error on the part of the conductor, rail engineers quickly suspected foul play. They were right, but for reasons they would probably never have wagered.

It turns out that a fourteen-year-old computer whiz kid had created an infrared remote transmitter capable of controlling all the junctions on the transit line. The boy spent months studying the city's rail system to determine the best places to redirect trains in order to cause the most havoc and hacked the switches throughout the town to redirect trains on his command.

In other words, the teen was able to use the city's tram system

as his "personal toy train set" by hacking and electronically commandeering the city's transit infrastructure. The teen was believed to have utilized the device on numerous occasions, and when he was caught and arrested, he admitted, like Mat Honan's hacker that he had carried out his act "just for the lulz" of it all.

But this prank resulted in the derailment of four trains and could easily have led to passenger deaths, an important distinction that left many security analysts fuming that more wasn't being done to ensure the safety of the city's critical infrastructure. They fittingly reasoned that if a fourteen-year-old boy, acting alone, could hack the transit system's network and wreak this sort of havoc for his own amusement, what was to stop criminals, terrorists, or a warring nation from doing the very same?

A Vulnerable Global Information Grid

We've seen how easy it is to hack into the majority of computer systems and how quickly it can be done. Mat Honan's experience proved that our digital lives can be struck from the record in an instant. T.J. Maxx and Citibank both learned the hard way what can happen when criminals thousands of miles away bring you into their sights. Given the obvious dangers, one would have thought a measure of prudence would be in order before adding everything that plugs into the wall or has a battery to the global information grid, yet we proceed full steam ahead in our growing love affair with all things tech.

As a result, we are increasingly connected to computer systems in ways we don't understand. Moreover, these connections are wholly untrustworthy and vulnerable—a poor foundation upon which to build the information society of the twenty-first century. Yet that is exactly what we are doing. Not only are our personal and work computers deeply enmeshed with the Internet, but so too are all of the critical infrastructures upon which our modern society depends. The electricity grid, gas pipelines, 911 dispatch systems, air traffic control, the stock market, our drinking water, streetlights, hospitals, and sanitation systems are all dependent on technology and the Internet to function. In this brave new world,

we've taken the human being out of the loop and have entrusted the backbone of civilization to machines.

The credit card transactions, point-of-sale payment terminals, and ATMs that keep the global flow of commerce and capitalism humming would come to a screeching halt without the computers to run the network. Computers decide how, where, and when to route electricity to ensure the power grid's stability. Computer-aided dispatch systems keep track of police cars, ambulances, and fire trucks so dispatchers know who is available and closest to respond in case of emergency. For a sneak peek of what this dystopian world without computers and electricity looks like, one need only turn on the television for a taste of techno-Armageddon-cum-zombie apocalypse from shows such as *The Walking Dead* or from films like *Planet of the Apes* and *Live Free or Die Hard*. Hollywood machinations aside, our computer-based critical information infrastructures are increasingly under attack and deeply vulnerable to systemic failure—the impact from which could be truly catastrophic.

Much of the world's critical infrastructures utilize supervisory control and data acquisition (SCADA) systems to function. SCADA systems “automatically monitor and adjust switching, manufacturing, and other process control activities, based on digitized feedback data gathered by sensors.” These are specialized, and often older, computer systems that control physical pieces of equipment that do everything from route trains along their tracks to distribute power throughout a city. Increasingly, SCADA systems are being connected to the broader Internet, with significant implications for our common security. Unfortunately, these systems were not designed with security in mind and were not engineered to be resistant to an Internet-connected world. The problem is worse than you think: in a July 2014 study of critical infrastructure companies across multiple sectors, nearly 70 percent of them had suffered at least one security breach that led to the loss of confidential information or the actual disruption of operations during the preceding twelve months.

What might a hacker do with access to these systems? Take, for example, the complex information technology systems regulating the local water treatment facility. The SCADA system consistently measures and adjusts the appropriate mix of chemicals to clean our

water and make it safe to drink. But what if such a system were hacked? Could the wrong amount of chemicals be mixed in, poisoning our water rather than purifying it? It may sound like fantasy, but hackers have already reportedly carried out an attack against the South Houston, Texas, Water and Sewer Department, according to a BBC report from 2011. The Internet protocol address of the attacker was traced to Russia, and the hackers involved were said to have repeatedly turned on and off a pump, quickly causing it to fail. While nobody fell ill in the attack, the proof of concept has been demonstrated.

What other infrastructure hacks might be possible? As it turns out, the sky's the limit, as the Federal Aviation Administration's control tower in Worcester, Massachusetts, found out all the way back in 1998. There a local teenager used his knowledge of computing to sever communications between inbound aircraft and the tower and even turned off the runway lights for approaching aircraft. While nobody was killed in the incident, the potential for disaster is obvious. Of course there have been many more attacks against critical information infrastructures around the world. One of the earliest occurred in Maroochy Shire, Queensland, Australia, in 2001, wherein a hacker attacked a sewage treatment plant. He gained control of the facility's industrial control systems and "caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel." The attack destroyed significant amounts of local marine life and flora alike, to say nothing of the environmental threat to local residents.

Perhaps one of the most critical systems vulnerable to attack is our national electricity grid. Without electricity, all the fineries of our modern world cease functioning—no lights, elevators, ATMs, traffic control, subways, garage doors opening, refrigerators, and pumping gas. And when the backup batteries and emergency generators inevitably die, no cell phones and no Internet. Despite our vital dependence on electricity as the technological infrastructure most central to our contemporary lives, the former U.S. secretary of defense Leon Panetta noted, "the next Pearl Harbor that we confront could very well be a cyberattack that cripples" our power systems and our grid.

Panetta's concerns seemed validated and further bolstered by

a report by the U.S. Department of Energy which noted that the American energy grid—often called the most complex machine in the world—connects fifty-eight hundred individual power plants and has more than 450,000 miles of high-voltage transmission lines. Yet 70 percent of the grid's key components are more than twenty-five years old. Each of these components uses much older SCADA technologies that are readily attackable and persistently targeted.

An investigation by the House Energy and Commerce Committee revealed that "more than a dozen American utility companies reported 'daily,' 'constant,' or 'frequent' attempted cyber-attacks ranging from phishing to malware infection to unfriendly probes. One utility reported that it had been the target of more than 10,000 attempted cyber attacks each month." The report concluded that foreign governments, criminals, and random hackers were all hard at work either planning or attempting to take down the grid. The findings build upon prior statements by intelligence officials to the *Wall Street Journal* confirming that cyber spies had "penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system." The report concluded that to say that spies from Russia and China have allegedly mapped the American grid so that in times of crisis or war with the United States its entire electrical network "could be taken out."

Terrorists also have designs on digitally attacking America's infrastructure. In the summer of 2012, a video from al-Qaeda's As-Sahab media wing was uncovered by the FBI. In the video, the terrorist organization called for its "'covert mujahidin' to carry out waves of cyber attacks against the U.S. networks of both government and critical infrastructures, including the electric grid." Earlier FBI investigations revealed numerous instances of al-Qaeda's conducting online target research and surveillance on emergency telephone systems, electric generation plants, water distribution facilities, nuclear power plants, and gas storage networks in the United States.

The terrorist organization had even completed elaborate targeting packages on potential critical infrastructures to be attacked, including photographs of intended targets, detailed notes, and online research.

Hackers too are working to understand, expose, and exploit

vulnerabilities of SCADA and other critical information infrastructure. At the Chaos Communication Congress, an annual hacker gathering held in Germany, analysts at Positive Research demonstrated how to get full control of industrial infrastructures in the gas, chemical, oil, and energy industries. Equally troubling is the fact that hackers share this information with each other and have even created fully searchable public databases of known exploits that can be used to commandeer critical infrastructures. One well-known hacker database, Shodan, provides tips on how to exploit everything from power plants to wind turbines, searchable by country, company, or device, providing detailed how-tos and greatly lowering the technical bar and knowledge for any rogue individual to hack our critical infrastructures. In effect, for attackers interested in gaining control of our connected world, Shodan has become their Google—one that is near impossible to shut down because Shodan is hosted on multiple servers in foreign countries around the world and publishing vulnerabilities is not currently a crime in most of these places.

Organized crime groups are also turning their attention to infrastructure attacks as a logical means of extorting money from utility companies and governments. Several such incidents reportedly occurred in Brazil between 2005 and 2007, when a wave of cyber attacks was carried out north of Rio de Janeiro and in the state of Espírito Santo. In that incident, nearly three million people were stuck in the dark when the local electricity provider failed to meet the extortion demands of a local crime syndicate. As a result, the city of Vitória, one of the world's largest iron ore producers, had numerous plants forced off-line, costing the company nearly \$7 million. The attacks were confirmed by U.S. intelligence officials, security researchers, and even obliquely by President Obama when he noted, "We know that cyber intruders . . . in other countries . . . have plunged entire cities into darkness."

WHOIS It?

The famous Chinese general Sun Tzu, author of *The Art of War*, cleverly observed twenty-five hundred years before the creation of

the Internet that "if you know thy enemy and know thyself, you will not be imperiled in a hundred battles." Accordingly, in order to understand the vast technological threats before us, we must understand our enemies. Each has different means and motives, but what they have in common is the risk each poses to our profoundly interconnected world.

The cast of characters responsible for cyber malfeasance is vast and includes nation-states, neighborhood thugs, transnational organized crime groups, foreign intelligence services, hacktivists, military personnel, cyber warriors, state-sponsored proxy fighters, script kiddies, garden-variety hackers, phreakers, carders, crackers, disgruntled insiders, and industrial spies. Each plays its role in what the U.S. military has declared to be the "fifth domain" of battle: cyberspace (following the militarization of land, sea, air, and space of generations past).

These parties frequently use similar tactics, albeit with varying degrees of sophistication. Yet all attackers benefit from the asymmetric nature of the technology: the defender must build a perfect wall to keep out all intruders, while the offense need find only one chink in the armor through which to attack. Among the factions battling in the cyber underground, there is cooperation, witting and unwitting, as the players often learn from and imitate the operational success of one another. For example, transnational organized crime groups use highly sophisticated reconnaissance operations to plan their attacks but often rely on neighborhood thugs to carry out elements of their plots, such as the placement of ATM skimmers, money laundering, or the fencing of stolen goods on eBay. Terrorist organizations learn from cyber criminals and hack for financial gain to fund real-world operations. Patriotic bands of citizens are often formed into cyber posses by their state-sponsored benefactors in nations such as China, Russia, and Iran and receive tacit approval, funding, and training. In doing so, they share some of the same techniques and tools with their government patrons. There is a symbiosis in the cyber underground and a commonality of methodologies across the full spectrum of threat actors.

Perhaps the first vision to come to mind when thinking of a hacker is the stereotypical image of a teenage male living in his mom's basement, pounding away at the keyboard, surrounded by

empty bags of Fritos and discarded Coke cans, trying to change his grades on his high school's computers (as did Matthew Broderick in the 1983 film *WarGames*). In the early days of hacking, it was the telephone system that was the target of hackers' attention as so-called phone phreaks manipulated the network to avoid the sky-high costs of long-distance calls. Let's not forget two hackers who spent part of their youth back in 1971 building "blue boxes," devices capable of hacking the phone network and making free calls: Steve Wozniak and Steve Jobs. The pair sold blue boxes to students at UC Berkeley as a means of making money that would effectively help fund their other small start-up, the Apple computer company.

As time passed, other notable hackers emerged, such as Kevin Mitnick and Kevin Poulsen. Mitnick famously broke into the Digital Equipment Corporation's computers at the age of sixteen and went on to a string of such cyber intrusions, earning him the FBI's ire and the distinction of being "America's most wanted hacker." Poulsen's ingenious 1990 hack allowed him to commandeer all of the telephone lines of a local Los Angeles radio station to ensure he would be the 102nd caller, thereby securing the top prize of a \$50,000 Porsche 944 S2.

These hacks from the 1970s, 1980s, and 1990s would seem benign by today's standards. In the intervening years, hackers have gone on to become highly organized and have formed global online crime syndicates. They commit identity theft, credit card fraud, health-care fraud, welfare fraud, and tax fraud. Organized crime groups are now going after bigger and more sophisticated targets as well, including the vast amounts of intellectual property created by businesses around the world, from a company's product plans to its computer source code. For example, in October 2013, criminal hackers targeted Silicon Valley's Adobe Systems, stealing thirty-eight million account log-ins and passwords as well as millions of credit card numbers (nothing new there). But what changed in that attack was that the criminals also stole more than forty gigabytes of computer source code for Adobe's flagship products, including Photoshop, ColdFusion, and Acrobat.

As a result, not only can criminals now freely sell Adobe products, but they could also alter the code and insert untold numbers of hidden back doors, malware, and additional exploits into the

product, causing Adobe's legitimate and unsuspecting customers to suffer widespread hacking attacks and identity theft—a troubling development indeed given Adobe's massive global footprint among computer users. Even Symantec, the maker of pcAnywhere and Norton AntiVirus, has had its source code stolen. Yep, the company that is selling you antivirus software to protect you from being hacked was itself compromised when a hacker stole 1.27 gigabytes of its security software source code and demanded a relatively paltry \$50,000 in exchange for not posting the data on the well-known hacker Web site The Pirate Bay.

Traditional organized crime groups, such as the Italian Mafia, Japanese Yakuza, Chinese triads, and Colombian drug cartels, have all diverted efforts and resources from their usual criminal activities to take advantage of the easy profits, greater anonymity, and limited police scrutiny afforded in cyberspace. Moreover, they do not have to worry about the draconian sentencing minimums often associated with their former economic activities, such as narcotics smuggling and trafficking in human beings. Organized crime groups in cyberspace are responsible for spam, phishing, fake pharmaceutical ads, the dissemination of child sexual abuse images, denial-of-service attacks, and extortion, to name but a few of their favored activities.

In addition to the stalwart old guard of organized crime, a more nimble class of pure-play cyber-crime organizations is exploding onto the scene. These newly emerging and professionally organized criminal hacking groups are highly profitable and truly global, with heavy concentrations in China, Indonesia, the United States, Taiwan, Russia, Romania, Bulgaria, Brazil, India, and Ukraine. New syndicates, such as the Russian Business Network (RBN) in St. Petersburg, have even made names for themselves as multi-product-line, full-service cyber-crime organizations.

RBN famously provides “bulletproof” Web site hosting services for all manner of other criminal enterprises and takes a completely hands-off approach to hosted content, freely welcoming anything from child pornography to malware exploit exchanges on its servers. Other professional criminal hacking groups, such as the ShadowCrew, offer online havens for “carders,” who specialize in the murky world of stolen personally identifiable informa-

tion, including forged passports and driver's licenses, and stolen credit cards—key ingredients in the world's growing identity-theft economy. ShadowCrew operated the now-defunct Web site Carder Planet.com, where over four thousand criminals from around the world could freely gather to buy and sell stolen and hacked identities, documents, and account numbers. Founded by the notorious criminal hacker Albert Gonzalez, ShadowCrew offered fellow criminals tutorials on everything from cryptography to card-cloning techniques, and Gonzalez's organization was reportedly responsible for stealing and reselling more than 180 million credit and ATM cards. The number and reach of these highly profitable transnational organized cyber-crime rings have grown, and the security intelligence firm CrowdStrike was actively tracking more than fifty such major organizations globally.

Besides transnational organized crime syndicates, hacktivists—politically motivated cyber attackers—represent one of the most influential and powerful groups in cyberspace. Anonymous, LulzSec, AntiSec, WikiLeaks, and the Syrian Electronic Army fall into this group and launch their attacks in retaliation for perceived injustices. Personalities such as Julian Assange, Chelsea (Bradley) Manning, and Edward Snowden have become household names for challenging some of the world's most powerful institutions and for releasing data that others would most certainly have preferred remain hidden. While Assange, Manning, and Snowden have been propelled onto the covers of newspapers around the world, other hacktivist groups prefer that their individual members remain discreetly hidden in subordination to the organization itself and its broader agenda. One such notable example is Anonymous, a self-described leaderless organization whose members have become recognizable in public for wearing Guy Fawkes masks.

The group's motto, "We are Anonymous. We are legion. We do not forgive. We do not forget. Expect us," manifests its organizational ethos: "The corrupt fear us. The honest support us. The heroic join us." When MasterCard, Visa, and PayPal all agreed to stop funneling donations to Julian Assange's WikiLeaks organization, Anonymous responded by launching a series of effective cyber attacks against the financial firms. Anonymous is strongly against what it perceives to be rigid antipiracy laws, and it took credit for

an earlier attack against the Sony PlayStation Network in response to Sony's support of U.S. antipiracy legislation known as the Stop Online Piracy Act.

Anonymous views itself as hacking for good and has taken on a wide variety of social causes, including its support of activists throughout the Middle East during the Arab Spring. Even some of the group's most ardent critics might find themselves supporting some of Anonymous's lesser-known activities in combating criminal organizations and injustice. For example, during an attack dubbed Operation Darknet, members of Anonymous targeted child pornography Web sites hosting vile images of young children being sexually abused. The hacker collective knocked the sites offline and released the names of fifteen hundred pedophiles using the services. Whether one supports or detests the actions taken by Anonymous and other hacktivist organizations, one thing is clear: they are a force to be reckoned with among the wide tapestry of threat actors in our über-connected world.

Hacktivism is capable of targeting any individual or corporation and can even have geopolitical impact the world over, as was seen during the Arab Spring. In recognition of their growing power, *Time* magazine ranked Anonymous as one of the hundred most influential people in the world in 2012. Their burgeoning influence and capabilities have not gone unnoticed by government, and it was recently revealed that the Government Communications Headquarters (GCHQ), the British equivalent of the American National Security Agency, had launched its own series of denial-of-service attacks against Anonymous and its membership in an effort to disrupt their activities. This dramatic response by the state against a non-state actor and hacktivist group demonstrates the impact Anonymous is having in the world.

Meanwhile, terrorist organizations too are increasingly using the Internet and other technologies to plan, support, and execute their murderous activities. Technology helps terrorists recruit new members in underground chat rooms, finance operations (through cyber crime or online fund-raising), communicate clandestinely, and disseminate propaganda, such as the gruesome beheading videos produced by ISIS (the Islamic State). ISIS is tech savvy and in its latest recruitment videos even edited in scenes from the video

game *Grand Theft Auto V* for effect. In its online video production, the reviled terror group offered new recruits the opportunity to "do the things you do in games, in real life on the battlefield... like attack a military convoy or kill police officers." The video is plastered with the ISIS logo.

Internet reconnaissance and research by terrorists are commonplace, and on more than one occasion officials have found Google Earth images of intended targets, including a 2007 planned attempt by terrorists to blow up fuel tanks at New York's John F. Kennedy International Airport. Terrorists have been early adopters of technology, particularly in their use of data encryption to secure their communications. For instance, "Ramzi Yousef, the convicted mastermind of the first World Trade Center Bombing in 1993, used encrypted files to hide details of his plot to destroy 11 U.S. airliners." In the Yousef case, it took law enforcement authorities more than a year to break the encryption algorithm used by the terrorist, and in doing so, police officials were fortuitously able to prevent the plot against the airlines.

Some counterterrorism experts have referred to the Internet as a "terrorist university," a place where terrorists can learn new techniques and skills to make them more effective in their attack methodologies. Widely available online are documents such as *The Mujahideen Poisons Handbook*, which contains various "recipes" for homemade poisons and poisonous gases. The six-hundred-page *Encyclopedia of Jihad* is also widely available online and includes chapters such as "How to Kill," "Explosive Devices," "Manufacturing Detonators," and "Assassination with Mines." In a striking example of how dangerous such online education can be, Dzhokhar Tsarnaev, the terrorist suspect convicted for his role in the April 2013 Boston Marathon bombings, admitted to authorities he and his brother learned how to make the pressure-cooker bomb used in the attack after reading step-by-step instructions published in al-Qaeda's online magazine, *Inspire*, in an article titled "Make a Bomb in the Kitchen of Your Mom."

Not only are terrorists using the Internet for operational support and planning, but they have turned to both hacking and cyber crime as means of funding and carrying out their real-world terrorist operations. In June 2007, a U.K. terrorist cyber cell was

disrupted by police when three British residents, Tariq al-Daour, Waseem Mughal, and Younes Tsouli, were charged with using the Internet to incite murder. Evidence presented showed that the men had used hacked credit card accounts to purchase goods to assist fellow jihadists—items such as night-vision goggles, global positioning devices, airplane tickets, and prepaid mobile phone cards—for the purpose of providing direct tactical support for terrorist operations. “The trio reportedly made fraudulent charges totaling more than 3.5 million U.S. dollars and was in possession of a database containing nearly 40,000 stolen credit card accounts.”

Even the infamous 2002 Bali bombing mastermind, Imam Samudra from the al-Qaeda-linked terrorist group Jamaah Islamiyah, funded his attack, in which more than two hundred people were murdered, with the \$150,000 he obtained by hacking into Western bank accounts and credit lines. Samudra was technologically savvy and while in prison wrote an autobiographical manifesto containing a chapter titled “Hacking, Why Not?” In the book, Samudra shared his hacking and “carding” techniques with his disciples, encouraging them “to take the holy war into cyberspace by attacking U.S. computers, with the particular aim of committing credit card fraud, called ‘carding,’” to fund operations. Terrorists seem to be getting the message, and both the 2004 Madrid bombings at the Atocha train station, in which 190 people were killed and nearly 2,000 wounded, and the 7/7 London bombings, in which 52 civilians were slain and over 700 injured, were funded in whole or in part through hacking and credit card fraud.

As the technical hacking skills of terrorist organizations increase, so too does the amount of ill-gotten gains they are capable of generating online. For example, in late 2011, police in the Philippines working with the FBI uncovered a telephone hacking scam against AT&T that defrauded the company and its business customers of \$2 million. The Filipino hacking cell was working with Jamaah Islamiyah and funneled the millions back to a Saudi-based terror group that in turn funded the Pakistani-based Lashkar-e-Taiba, the terrorist group responsible for the deadly 2008 bombing siege that gripped the city of Mumbai, India, and killed and maimed hundreds.

It is clear that criminals, hacktivists, and terrorists use our

interconnectivity against us, whether for profit, politics, or mere sacre. They have schooled themselves in science and technology and have proven a formidable force in exploiting the fundamentally insecure nature of our twenty-first-century technological skin. Yet thieves, hackers, activists, and terrorists are not the sole inhabitants of the digital underground. They are accompanied by a phalanx of nation-states, cyber warriors, and foreign intelligence services, each handily playing in the so-called fifth domain, fully leveraging for their own purposes the insecurity of the underlying digital infrastructure that unifies the planet.

Though the average Internet user today may be busily updating his Facebook status or playing *Angry Birds*, it is important to recall that today's Internet was born of the Defense Advanced Research Projects Agency (DARPA), a U.S. Department of Defense research institution created to ensure redundancy in military communications in the event of nuclear attack. The Internet is a military creation with significant corollary geopolitical ramifications.

It is when governments turn their attention (and budgets) to offensive cyber operations that we can see the full range of vulnerabilities in the hardware and software upon which we depend and that our common technological frailty is fully exposed. Though a \$50,000 criminal extortion demand against Symantec or even a \$1 billion hacking loss at Target remains noteworthy and surely merits our attention, it is chump change compared with the computer spying breach of the Pentagon's \$300 billion F-35 Joint Strike Fighter project—the most expensive Defense Department weapons program in history.

In May 2013, the U.S. government specifically named China as being responsible for a series of hacks against vital American defense and government systems, including the F-35. Over the years, it has been reported that many other defense blueprints and technologies have been stolen, including those from an advanced Patriot missile system known as PAC-3, the navy's Aegis Ballistic Missile Defense system, the F/A-18 fighter, the V-22 Osprey, the Black Hawk helicopter, and the littoral combat ship. According to an FBI report, China has secretly developed an army of 180,000 cyber spies and warriors, mounting an incredible ninety thousand computer attacks a year against the U.S. Defense Department net-

works alone. The totality of the thefts and their impact on American national security are breathtaking.

China's purported cyber-hacking activities provide it with significant strategic advantages, including an immediate tactical and operational edge in any conflict with the United States. Having the blueprints to so many U.S. defense systems provides key details on how they work and importantly how to defeat them in times of crisis. Moreover, this great "brain robbery" saves China billions in research dollars from its own military development costs (and decades of work) by merely appropriating and building upon work paid for by American taxpayers.

Of course it is not just the American military's technology that is being targeted by China, but rather a litany of Washington institutions, including law firms, think tanks, human rights groups, contractors, congressional offices, embassies, and any number of federal agencies. Moreover, a 2009 report by Canadian researchers at the Infowar Monitor, the SecDev Group, and the Citizen Lab at the University of Toronto uncovered the so-called GhostNet, "a vast global cyber espionage network" extending to 103 countries that was controlled by servers in China and targeted the Tibetan government in exile and the Dalai Lama himself.

China has also been accused of hacking numerous media outlets, including most famously the *New York Times* in early 2013 after the paper reported that the relatives of China's prime minister, Wen Jiabao, had accumulated billions of dollars of wealth through their business dealings since Wen had entered office. The breach gave the perpetrators access to any computer on the *New York Times's* network, and it was believed the Chinese were working to uncover sources and contacts that might damage the reputations of China's leaders. The *Times* hired the private cyber-security firm Mandiant, which investigated the incident and in a fascinating report tied the attack back to Unit 61398 of the People's Liberation Army. The unit's headquarters, on Datong Road in the Pudong district of Shanghai, is a 130,000-square-foot, twelve-story building in which thousands of employees go to work every single day hacking governments, companies, and individuals around the world.

Those technological thefts that are not directly carried out by the Chinese state itself are often sponsored by the state and per-

formed by appointed proxies, with profound implications and deep costs for businesses around the world. In 2012, *Bloomberg Businessweek* covered China's ongoing theft of global intellectual property in a cover story that screamed in full-page letters, "Hey China! Stop Stealing Our Stuff." The piece featured the tale of Dan McGahn, the CEO of the Massachusetts-based American Superconductor (AMSC), a green energy technology company specializing in the design of power systems and the software that runs large wind turbines. In March 2011, AMSC's largest customer—China's formerly state-owned Sinovel Wind Group—suddenly began refusing shipments at its assembly plant in Liaoning province and canceled more than \$700 million of pending orders from AMSC. The market's response to AMSC's canceled orders was brutal: a 40 percent drop in valuation in a single day and an 84 percent decline by September of that year.

An investigation into the matter revealed that Sinovel's own turbines "appeared to be running a stolen version of AMSC's software" and that the Chinese firm had snatched a complete copy of the American company's proprietary computer source code. Because Sinovel had in its possession all of AMSC's intellectual property, it no longer needed AMSC or its products and could merely produce AMSC's products itself. As a result, the Chinese company canceled its existing supply contracts worth more than \$700 million with the Massachusetts firm.

All told, between thefts of commercial, governmental, and military intellectual property, China's hacking efforts have netted the nation the greatest transfer of wealth in human history. According to Akamai's *State of the Internet* report, China is the source of a shocking 41 percent of all of the cyber attacks in the world. Of course China vehemently and routinely denies involvement in any global hacking activities. When allegations arise, responses typically come from a Chinese embassy spokesman in the capital city of the hacked country in question, whether Paris, Berlin, or New Delhi. A message issued by a Chinese embassy official named Wang Baodong in Washington, D.C., is typical of their response: "China is firmly against international hacking activities and is ready to work with other countries to secure the cyberspace." Wang's denial is hardly the first time such a response has been issued: a Google

search for the phrase "China denies hacking" yields a mere thirty-five million such denials.

Though China is the most populous nation on earth, it is not the only country to engage in cyber operations. According to the former FBI director Robert Mueller, there were at least 108 nations with dedicated cyber-attack units going after industrial secrets and critical infrastructure alike, including Iran. In late 2012, a previously unknown hacker group called Cutting Sword of Justice took responsibility for carrying out the most destructive computer sabotage against a company to date when it targeted the oil and gas giant Saudi Aramco. The offensive took place on the eve of one of the holiest nights in the Islamic calendar, Lailat al-Qadr, the day Muhammad is said to have revealed the Koran to his followers and when Aramco's fifty-five thousand employees stayed at home to celebrate with family and friends. At stake, 260 billion gallons of oil, valued at over \$8 trillion (fourteen times the market cap of Apple Inc.).

During the incident, an unknown insider with access to the facility inserted an infected USB thumb drive into a single PC connected to the company's computer network. Within minutes, the drive's viral payload, known as Shamoon, was spreading like wildfire across all of Aramco's thirty thousand corporate computers. Though its goal was to disrupt oil and gas production at Aramco's facilities, good security practices meant that the virus "only" destroyed corporate data. The toll? Shamoon erased 75 percent of the company's thirty thousand corporate hard drives, wiping out "documents, spreadsheets, e-mails, files—replacing all of it with an image of a burning American flag."

The Cutting Sword of Justice claimed its attack was in response to Saudi "crimes and atrocities" in Syria and Bahrain against Shiite protesters. American intelligence officials suspect that the Cutting Sword of Justice is nothing more than a front for Iran, which they believe was to blame for sponsoring the attack. The shocking capabilities demonstrated in the Aramco attack predated several other successful attacks by the Iranian government, including a series of distributed-denial-of-service (DDoS) disruptions in early 2013 targeting the American financial services industry. Numerous marquee banks, including JPMorgan Chase, Bank of America, Wells

Fargo, BB&T, HSBC, and Citigroup, were affected by the attack, which made their corporate networks and public Web sites inaccessible for extended periods of time and prevented customers from accessing their money. A hacker group calling itself Izz ad-Din al-Qassam Cyber Fighters claimed responsibility for this cyber blitz, but American officials say the group is merely a proxy for Iran.

The widespread denial-of-service attack against America's financial industry by Iran was shocking for its size and scope and for the massive volume of data generated by the perpetrators. "Some banks were hit with a sustained flood of traffic that peaked at 70 gigabits" per second. To put that volume of DDoS traffic in perspective, it is as if 1 billion people simultaneously phoned your bank, hung up, and immediately dialed back one second later. In order for your call (or visit to its Web site) to get connected, you would be number 1,000,000,001 on the list to get through. In other words, for all intents and purposes, you would never reach the bank.

Strikingly, the Iranian-backed attack against the financial services sector was reported to be multiple times larger than the infamous 2007 attack against the nation of Estonia by Russian-based hackers—an attack that nearly knocked the small Baltic nation entirely off-line. The incident is widely believed to have been carried out with the direct support of the Russian government via nationalist proxy hackers after Estonia decided to move a Soviet-era grave marker from its long-standing position in Tallinn's city center to the outskirts of town—a move that deeply offended Moscow. Many security experts called the all-out digital assault against Estonia the "world's first cyber war" because of its size and scale. Given that Iran had just bested that attack, one security researcher noted the Islamic Republic's technical bombardments have graduated from being the equivalent of "a few yapping Chihuahuas into a pack of fire-breathing Godzillas."

Of course, there have also been widespread allegations of hacking by the United States against the rest of the world, based largely on the numerous classified documents stolen and unilaterally released by the former National Security Agency (NSA) contractor Edward Snowden beginning in June 2013. Snowden detailed at great length the global technical surveillance apparatus run by the National Security Agency and provided documentary

evidence to support his claims in discussions with the journalists Glenn Greenwald and Laura Poitras. Programs such as PRISM and XKeyscore subsequently came to light, as did the NSA's purported ability to track billions of e-mails, phone messages, chat sessions, and SMS texts each and every day.

While living in Moscow, Russia, under temporary asylum status, Snowden continued to catalog U.S. offensive cyber and technical operations, including the tapping of the personal mobile phones belonging to world leaders ranging from the German chancellor, Angela Merkel, to the Brazilian president, Dilma Rousseff. Moreover, Snowden divulged that millions of citizens in ally nations such as France and Germany were having their communications recorded, to the tune of 120 billion calls a month around the world. Snowden's leaks also served to limit international sympathy for U.S. complaints regarding intensive cyber operations by the People's Republic of China, especially when he revealed that America too had launched cyber operations against Chinese targets, including China Mobile and the prestigious Tsinghua University. Depending on one's political beliefs and point of view, Snowden is either an enemy of the state, a hero, a whistle-blower, a dissident, a traitor, or a patriot. Most feel strongly one way or another. Regardless of how history judges Snowden, his disclosures, if true, paint a highly detailed portrait of how governments are entering the cyber fray.

An analysis of the threat-actor landscape in cyberspace reveals hackers, criminals, proxy warriors, terrorists, and rogue governments, all fully capable of exploiting the insecurity of the technological infrastructure of our world. Our financial data, identity, children's baby pictures, and power grids are all vulnerable and at risk, easy targets for the picking. Yet for as ubiquitous as technology seems in our lives today, the exponential rate of growth means that just over the horizon is a tidal wave of technological advances that will leave our heads spinning. Not only will the breadth and depth of our connection to the global information grid vastly expand, but new technologies heretofore relegated to the realm of science fiction will soon emerge as science fact. In short, we ain't seen nothing yet.