SKATING ON STILTS

Why We Aren't Stopping Tomorrow's Terrorism

Stewart A. Baker

HOOVER INSTITUTION PRESS
Stanford University Stanford, California

9 Moore's Outlaws

In the years since 9/11, we had done a lot to meet the challenge posed by the exponential growth of international travel. Our border procedures weren't airtight, of course; they never had been. But we weren't flying blind, making decisions at the border on thirty seconds of chat and intuition, either. We'd come a long way, and while we still had further to go, at least everyone understood how important it was to finish the journey.

The challenge posed by computer security was different. There had been no dramatic meltdown. Most people still scoffed at the idea that the exponential growth of information technology revolution could lead to disaster.

Yet for some of us, losses from the information technology revolution are already greater than the gains.

Just ask Howard Crank's widow.

Howard Crank lived a quiet life that revolved around his modest California duplex. He was seventy-three years old, after all, and he'd had both legs amputated above the knee due to diabetes. His wife's health was not good. He was living on his Air Force veteran's pension. But he could afford a computer, and he loved it. It helped him find old Vietnam buddies and research new charities to add to the three dozen he already supported. He might be halfway to housebound, but the new technology was a godsend. Thanks to Moore's Law and the Internet, the whole world was at his doorstep.[1]

The Internet, it appears, is how he discovered that he'd won $715,000 in a Spanish lottery. Money was tight on an Air Force pension, so this was amazing news. Of course, it turned out that there were transfer taxes for him to pay before the winnings could be sent to him. It grew expensive, but his share of the lottery was also growing—to $115 million.

Howard Crank's life savings were $90,000. Bit by bit, he sent it all.

It wasn't enough. He got calls from Spain, explaining the hassles and delays. He mortgaged his home and sent the proceeds. More calls. When he wondered aloud whether he'd ever see the money, the caller asked him to have faith. They prayed together.

A few weeks later, he took out a second loan on the house. He maxed out two credit cards. All the money, perhaps $300,000 in all, went to Spain. Even that was not enough to break his lottery winnings free. He asked his stepdaughter for $40,000. He didn't want to explain why.

She thought that was odd. So when he was hospitalized a few weeks later with a broken thigh, she checked his financial records. She found that Howard Crank had ruined himself and his wife in an apparent Internet hustle. The Spanish scam artists disappeared without a trace. Crank died of a heart attack before he could explain how it happened.

"I think he probably knew it was a fraud at the end," his stepdaughter told me. "But he was hoping against hope. He'd sent them so much money already, and they were so convincing. But by the end he'd lost his zest for life. He was so desperate."[2] Desperate he should have been. He had not just squandered his own assets. A year after his death in early 2010, his widow had lost her home and been forced into bankruptcy by the debts he left behind. "She's had to move in with us. She's starting over again at the age of eighty," her son-in-law told me.[3]

Howard Crank would never have let a con man into the quiet life he and his wife were living. But the Internet that brought the world to his doorstep brought the world's con men as well. Information technology

empowered Howard Crank to search the world for old buddies. And it empowered fraudsters to search the world for the handful of people who might be ripe for their scam.

For Howard Crank, the exponential growth in information technology turned out to be a disaster. It was great for a while. He loved what the new technology did for him, and how cheaply it performed its miracles. But in the end, nothing he gained by embracing it was worth what he lost.

Will the rising curve of information technology eventually leave the rest of us where it left Howard Crank? You're probably thinking that Howard Crank, sympathetic as his story may be, just wasn't savvy enough. You would never fall for such a scam. And you will never suffer the harm that he did.

Well, don't be so sure. The science fiction writer William Gibson once declared that, "The future is already here. It's just unevenly distributed."[4] He was thinking of the wonders of new technology, but bad futures are distributed as unevenly as good ones. And Howard Crank may have been in the vanguard of Americans ruined by information technology.

Thanks to information technology, it is now cheap to screen millions of people to find those who were susceptible to the lottery fraud. That same technology will make it cheap to screen the world for people and machines that are susceptible to other forms of fraud as well. You may not fall for the Spanish lottery, but you're probably susceptible to *something*. And even if you aren't, your machines are.

Are you really sure the fraudsters won't find you in the end?

Exponential technologies always seem to serve dessert first. That's why they grow exponentially. Their benefits are immediate and irresistible, so we use them in numbers that double and double again. In the beginning, it seems implausible that they will be misused. Indeed, at the outset, people do use them mostly in good, socially responsible ways. I leave it to the philosophers whether that's because people are

basically good or because it takes time for people to figure out how to be bad using new technologies.

Whatever the reason, information technology certainly followed the same path as commercial jets. It took decades between the time the technology was first democratized and the first really frightening misuse.

Until the late 1980s, the risks of misuse were almost entirely theoretical. Computer viruses had been invented by then, but mainly just to show how they would work. It wasn't until the mid-1980s that "wild" computer viruses began to spread from one PC to another via floppy disks. Then, in 1988, a worm caused much of the Internet to grind to a halt. For the academic and defense users who then dominated the Internet, the worm was a shock. But they relaxed when they found that the worm's author, Robert Morris, wasn't a spy or a criminal. He was a student, and he claimed he'd been testing a concept that got out of control.

In retrospect, what's most notable about the malware of that era is its comparative innocence. It caused damage, sure. But it was either academic or nihilistic in purpose; it demonstrated the capabilities and perhaps the ill will of the author. It wasn't really much of a threat, although the worst examples could destroy stored data.

Most attacks were the digital equivalent of the Plains Indians "counting coup" by striking an enemy with a stylized stick and escaping. Like counting coup, the purpose of early hacking was to gain prestige—more by demonstrating prowess rather than by causing harm. And computer security only needed to be good enough to outfox adolescent malcontents, a task both industry and government felt fully capable of handling.

By the mid-1990s, though, the Internet had become a fully democratized place, and money had replaced showing off as a motive for hackers. Spam was the earliest form of profitable Internet crime. And when network administrators started blocking spam by refusing to accept mail from spammers' machines, hackers found they could compromise other people's computers in bulk, then use those machines

to send the messages. If the senders of unwanted email were widely distributed, spam couldn't be stopped by quarantining a few suspect computers. Hacking wasn't just fun anymore; it could put money in the hacker's pocket.

Once underground networks of compromised machines had been assembled, it turned out that they could be used for other profitable crimes as well. If all of the captured machines could be induced to send meaningless messages to a single Internet site at the same time, the site would be unable to process them. The site would falter and fail. Legitimate users would be locked out.

Such "distributed" denial of service attacks turned into a new-style protection racket. Gambling sites, for example, simply cannot afford to be unavailable in the days and hours before the Final Four basketball tourney. If a site suffers an effective denial of service attack, there is a good chance that it will pay a reasonable "security" fee just to get back online quickly. That wasn't the only use to which criminals could put herds of zombie machines. The machines could be programmed to visit ad-supported websites and mindlessly click ads, earning illegitimate click-through fees for those sites.

But security professionals at large firms still had confidence in their defenses. Denial of service was a concern, sure, but the risk could usually be managed by retaining an ISP with lots of bandwidth and an ability to filter packets quickly. Distributed spam took away one tool for discouraging spam, but there were plenty of other ways to filter unwanted mail. For most users, spam was at worst a nuisance.

But malware continued to grow more sophisticated, and it could use the Internet to spread rapidly. Several viruses in 2000 and 2001 caught large companies unprepared and forced a shutdown of their networks while the viruses were eradicated. Hackers began to find ways to intrude into important financial and military systems.

This was getting serious.

Even so, most security experts thought the plague could be contained. They blamed systems administrators who didn't patch their systems quickly enough. Most of all they blamed Microsoft. The

company had emphasized new features over security, they complained, and in its drive to be first to market it had written sloppy code. Other operating systems were said to be more secure; and many thought that relying on a variety of operating systems was inherently superior to the "monoculture" created by Microsoft.

Stung, Microsoft fought back. Bill Gates himself took on the problem. Gates was famous for his insight into the future of the personal computer. Previous Gates messages had produced profound changes in Microsoft's strategic direction, most famously when he wrenched Microsoft into the Internet age, focusing the entire company on the challenge posed by Netscape—and leading to Microsoft's (temporary) victory in the browser wars.

By January 2002, Gates had a new focus. He announced that security was the key to Microsoft's future. From now on, all of its products would be built with security in their foundation: "When we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve."[5]

The email was a call to arms. All of Microsoft's employees were expected to bring this new focus to their jobs. In the past, a single-minded focus had enabled Microsoft to beat some of the most talented companies in the world. IBM, Lotus, WordPerfect, Ashton-Tate, Digital Research, Sun, Real, Apple, AOL, and Borland—not to mention much feared and rarely bested Japanese electronics makers like NEC and Toshiba—all had tried to stand between Microsoft and its strategic vision of the future. Microsoft had defeated them all.

Now Microsoft was gearing up for battle again. This time, though, it only had to beat a bunch of punk hackers. That should be a piece of cake. Once it was done, a new age of online security would dawn, with Microsoft's trusted products at the heart of every online transaction.

More than seven years have passed since Microsoft set out to beat a ragged band of hackers. The company has rewritten its operating

system more or less from scratch. And its code is indeed far more secure than in 2002.

But it has not won the war. The second Tuesday of each month still brings a boatload of corrections and patches that the company must make to even its newest and most secure operating systems. By 2009, the ragged band of hackers was looking a lot more sleek and prosperous than before, and Microsoft had suffered its first revenue decline in history.

More important than Microsoft's security failures are its successes—and how little difference they have made. Microsoft has indeed tightened up the operating system. But the structure of the PC world has made that almost irrelevant. The point of the PC is the control it gives to the user—who can decide what applications to run—and to the developers, who can create new applications quickly and easily. At the end of the day, Microsoft must empower users and developers. And so that's what its security approach does. Windows Vista, for example, was famous for nagging users to confirm their dangerous decisions to run new code or open new attachments—so famous that Windows 7 has had to cut back on the nagging, despite the security risks. The one thing Microsoft can't do is forbid users to make dangerous decisions. If Microsoft tried that, it would leave its users angry and looking for a new operating system. The same is true for applications; Microsoft can't require developers to write secure code without discouraging them from writing Windows applications. And if it does that, it loses its main advantage in the market—the overwhelming number of applications that run only on Windows.

So, to the extent that Microsoft has succeeded, it has simply displaced the risk. Online security is still getting worse, but it's getting harder to blame the operating system. Instead of exploiting the operating system, more and more attacks exploit holes in applications. Or they induce the user to do something he shouldn't do.

Or both.

One night in January 2009, at about the same time that Howard Crank was sending thousands of dollars to Spain, Beny Rubinstein was getting ready to turn off his computer and go to bed.

Suddenly he got an instant message from Bryan Rutberg, a friend who worked for a technology company. Rutberg's message got right to the point.

"Look, I really need your help."[6] Rutberg had taken a quick trip from Seattle to London, where he'd been robbed. He was broke in a foreign land. His Facebook page said the same thing, carrying an update that said, "Bryan NEEDS HELP URGENTLY!!!" Bryan needed a loan to get home. Could Rubinstein help?

Rubinstein could. He wired $600. That wasn't enough, so he sent another wire transfer—$1,143 in all.

In fact, Rutberg was still in Seattle. His Facebook account had been hacked, and the hacker was messaging Rutberg's friends, asking them all for quick wire transfers.

Rutberg, meanwhile, was locked out of his own account. He tried to stop the impostor by posting a comment on his own page, using his wife's account. Rutberg's comment was quickly deleted, and his wife was "unfriended." He had lost control of his online identity to a brazen scam artist.

A couple of days later, Facebook closed down the account, but Rubinstein's money is long gone. Neither Rubinstein nor Rutberg is a technological naïf. But both were defeated by the mass customization of online fraud. It's not hard to write programs that will look for weak Facebook passwords, or that will send urgent instant messages to the friends listed in compromised accounts. Only when someone responds to the messages do the scammers need to become personally involved. The marks are all prequalified.

Best of all, it's possible for the scammers to get in and get out in hours, then disappear halfway around the world. Local police are helpless; they "are not investigating this case," said a police spokesman. "It is pretty much at a dead end."[7]

As Microsoft has tightened the operating system, hackers increasingly rely on mass social engineering and insecure applications to open a hole in the victim's defenses. Facebook is, of course, free, and

the company is famous for not having a revenue model to match its massive user base. So it's not surprising that its site still has security problems. But it's the social engineering that made this scam work. Rutberg's friends may not trust strangers who tell them they've won the Spanish lottery, but they do trust him.

In fact, the combination of "authorized malware" and targeted social engineering is so powerful that, despite Microsoft's efforts, it's now easier than ever to compromise computers, and their networks.

No one can say we weren't warned. The United States government told us all that a computer security crisis was brewing. Twice, in fact, and under two different presidents.

President Clinton cautioned in January 1999 that, "We must be ready—ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks, police, fire, and health services—or military assets."[8]

A year later President Clinton proposed a series of measures to address the security problem.

Two years later, President George W. Bush created a special adviser on cybersecurity who spent a year developing a computer security strategy.

Neither effort made much headway. The public didn't see the problem. The network attacks that alarmed Washington were classified. Officials couldn't talk about them. Meanwhile, privacy and business interests worked overtime to persuade the public that national security concerns were overwrought. The real risk was government monitoring and government regulation, they insisted.

And, by and large, that was the view that prevailed—twice, and under two presidents. Nothing was done about computer security that anyone in the privacy or business lobbies might object to.

In 2009, a third president promised to make computer security a top priority, and shortly after taking office, the Obama administration also produced a security strategy. Once again, though, the strategy lacked punch. It failed to call for any action that could possibly irritate

business or privacy groups. It spoke of cybersecurity only in alarmed generalities, unable to explain why Americans should be concerned enough to suffer even modest inconvenience.

But this time may be different. Thanks to the work of a band of Canadian security researchers, we now have a remarkable—and completely unclassified—insight into just how easily computer hackers can penetrate even carefully secured computer networks.

The young Tibetan girl waited quietly in line at the border. Call her Dechen, though that's not her real name. She had spent two comfortable years studying in Dharamsala, India. Now she was going home. She had made the long trip across Nepal to the border with Tibet. The border crossing made her uneasy, but she told herself the Chinese border guards had no reason to stop her.

Dechen was a follower of the Dalai Lama, and she had spent much of her time in India conducting computer chat sessions with his supporters inside China. But she had been careful. She really had been a student. There was no way the Chinese government could know what else she had done. Or so she hoped.

Dechen stepped forward and presented her identification to the guards. They looked it over with care. Too much care. Something was wrong. Her heart sank. She was under arrest.

She was sent to a detention center. No one would tell her why. Could she have been compromised somehow in Dharamsala? She couldn't understand it.

Finally, after two months in captivity, she was called to the interrogation facilities, where two plainclothes officers immediately began questioning her about her activities on behalf of the Dalai Lama. She denied the charges, clinging to her story.

"I was a student. They cannot know what else I did," she must have told herself.

But over and over, intelligence officers accused her of working for the Dalai Lama's youth group. Over and over, she denied it. She had gone two months without contact with friends or relatives, but if she

held firm, they would have to let her go. She stuck to her story.

Finally, the officers lost patience. They pulled out a thick file. The folder held a full transcript of her online chat sessions. It covered years. They'd known everything, recording it as she typed. They told her the names of all her coworkers. All the attempts at security, all the work of the Dalai Lama's youth group, had been defeated.

Dechen was devastated. But the officers were more interested in sending a message.

—Go back to your village, they said, and tell your coworkers that we know who they are. They are not welcome in China anymore. They can expect the same treatment you got, or worse, if they return.[9]

It was over.

The Office of His Holiness the Dalai Lama is partly a religious, partly a diplomatic mission. The Dalai Lama travels widely and seeks audiences with foreign diplomats and officials to demonstrate support for his faith and for Tibetan autonomy. The Chinese government in turn vehemently opposes autonomy for Tibet and does all it can to discourage official meetings with the Dalai Lama.

The Dalai Lama's travel schedule is thus a matter of high state interest, and the planning of his meetings has an element of cat and mouse about it. The Dalai Lama's office finds that the best way to set up those meetings is first to send an email to the officials the Dalai Lama hopes to meet and then follow up quickly with a telephone call.

But around the early part of 2008, something odd began to happen. The Dalai Lama's office would send an email to a diplomat as usual, proposing a meeting. Then it would call to discuss the details, again as usual. But the diplomat's office would be strangely cool. "We've already heard from the Chinese government," the diplomat's staff would say, "and they've strongly discouraged us from having this meeting."

The Dalai Lama and his office had been using the Internet since the 1990s. His network administrators know the risks, and they've been careful about computer security for years. They'd implemented the

standard defenses against network attacks. They didn't know what had happened. But the evidence of a serious breach was simply too strong.

They called in a team of Western computer security experts. What the experts found was deeply troubling, and not just for the Dalai Lama.

Some of the Dalai Lama's staff participate in Internet forums. They chat with other, like-minded individuals about the Dalai Lama's goals and activities. Sometimes one of their online acquaintances sends them Word or .pdf documents relevant to those activities.

The experts concluded that hackers had monitored these forums and then forged an email from a forum participant to a member of the Dalai Lama's staff. Attached to the email was a document of mutual interest. When the staff member opened the document, he also activated a piece of malware packed with it. While the staff member was reading the document, the malware installed itself in the background.

The malware was cleverly designed; two-thirds of commercial antivirus software programs would have missed it. (Hackers often subscribe to antivirus software so they can test their malware against it at leisure.) Even if one attachment were stopped, it would be a simple matter to retransmit the message using a different bit of malware; the attackers could keep trying until something got through.

Once installed, the malware would "phone home," uploading information about the victim's computer and files to a control server operated by the hackers. Next, the captured computer would download more malware to install on the staff member's machine. This was often a complete administrative program that would allow the attackers to control the staffer's computer, and in some cases the entire network.

The administrative malware took full advantage of the empowerment made possible by today's technology. It featured a graphic interface with dropdown menus offering even an unsophisticated attacker a wide variety of options.

Want to record every keystroke as the user types so you can steal all his passwords? Check one of the options on the menu.

Want to turn on the user's microphone, turning it into a bug so you can listen to the office conversations? Check another box.

Want video straight from the user's desktop camera? That's just another option on the menu.

In the end, the Dalai Lama's office was living a version of Orwell's *1984*. Telescreens in each room spied on the occupants. But in this version of *1984*, Big Brother didn't even have to pay for this spy equipment. It had been purchased and installed by the victims.

Once the hackers had compromised a single computer on the network, it wasn't hard to compromise more. Every time an infected computer sent a document by email, malware could be attached to the file. The recipient couldn't possibly be suspicious; the email and attachment were exactly what he expected to receive from his colleague. He opened the document. The malware installed itself in the background. The cycle began again. It was an entire network of surveillance, dubbed Ghostnet by the security team.[10]

Ghostnet has lessons for all of us. You may be sure you wouldn't fall for the Spanish lottery, and perhaps not even for a Facebook call for help, but it's hard to find any comfort in this story.

Do you rely on standard commercial antivirus software to scan attachments? Do you open documents sent by people you've met online? How about documents from prospective customers or clients? Or old friends you recently connected with online? Do you open mail and documents sent to you by coworkers?

Of course, you do. So do I. And that means that most of us are no more able to defend ourselves from this attack than the Dalai Lama was.

If there were any doubts about the scope of such attacks, they were eliminated by what the security team did next.

They took another look at the IP address of the hacker's control server, and asked a simple question.

"Do you think hackers who need a graphic interface to steal secrets are really good at locking down their own computers?" I imagine the Canadian team sharing a mischievous smile as they asked.

Perhaps a veil should be drawn over exactly what they did next. Hacking is illegal in most jurisdictions, even if you're hacking someone who has just hacked you. Using methods they decline to specify, the security team was able to verify that whoever attacked the Dalai Lama's network was indeed much better at breaking into other people's computers than at keeping intruders out of their own.

Finding themselves inside the hackers' control servers, the security team naturally had a look around. They watched as reports came in from the Dalai Lama's computers. But that's not all. Reports were coming in from other computers as well. Hundreds of them.

The hackers who compromised the Dalai Lama's network were collecting data from nearly thirteen hundred other computers. Who else had been targeted by the attackers? That wasn't hard to find out. All the security team had to do was to ask who owned the IP addresses of the compromised computers.

What they found was a Who's Who of Asian organizations that ought to be highly concerned about—and pretty good at—computer security: Indian embassies in the United States, Germany, and the United Kingdom; the foreign ministries of Iran, Indonesia, and the Philippines; the prime minister's office in Laos. All were in thrall to the attackers' servers. Computers in sensitive businesses, from the Asia Development Bank to Vietnam's petroleum company, were also sending the attackers their data.

And, even though this set of attacks does not seem to have been aimed at the United States, Ghostnet was collecting reports from computers that belonged to the Associated Press and the auditing firm of Deloitte & Touche. Oh, and NATO too. In early 2010, Google announced that it and many human rights campaigners using Gmail had been targeted with the same attacks.

No one was safe.

The security team split on the question of whether to assign responsibility for Ghostnet to China. Some said it must be the Chinese government. Others were willing to let the facts speak for themselves. The Chinese government denies everything.

But there's not much comfort for us in the denials. The attacks happened, and they worked. If a government wasn't responsible, then this kind of capability is already in the hands of organized crime. Indeed, with its script-spy graphic interface and unsecured control servers, the whole episode underlines a troubling fact. Thanks to exponential empowerment, today's hackers don't even have to be very good. Empowered by democratizing technology, they can still beat our best defenses.

In fact, something similar to Ghostnet is already being used by organized crime. Most businesses depend on bank clearinghouse accounts or electronic fund transfers to pay their bills. They log on to bank sites using passwords; for larger amounts they may also be asked a set of "challenge questions" seeking information only the businesses know. But corporate officials also open email attachments from business contacts, and once attackers have access to the officials' keystrokes, neither the password nor the challenge questions offer any security. Hackers have stolen more than $100 million from U.S. businesses using this technique, the FBI reported in October 2009.[11]

I wasn't in government in 1998 or 2003, when the Clinton and Bush administrations called for new computer security measures. I didn't get the classified briefings that galvanized both presidents. Now I figure I don't have to.

This is scary enough.

But maybe you're not ready to agree. Maybe you're worried that these security alarms are a little too convenient—perhaps just an excuse for the government to spy on Americans and interfere with the economic engine of Silicon Valley. Surely, you think, there are still a few good defenses left.

Well, let's take a look at some of the top reasons that people think computer security risks can be managed successfully.

It's a Microsoft Problem. I know plenty of people who still believe that Microsoft's products are uniquely insecure, and that all we need to do is get Microsoft to clean up its act or take our business elsewhere.

For some, the security of Linux was an article of faith; its source code is open to inspection by anyone, so it is protected from exploit by all those watching eyes. And Apple, which didn't even offer an antivirus program for decades, was protected by, well, by Steve Jobs's sheer animal magnetism.

The last few years have been hard on those illusions. As Apple gained market share, malware authors began writing for its operating system, and they didn't have any trouble finding holes. It turns out that, according to a 2009 talk at the Black Hat security conference, even Apple's keyboards can be hacked to reveal all the user's keystrokes.[12] Apple now recommends that its users run multiple antivirus programs.[13]

And all those eyes on Linux's code? In August of 2009, two Google researchers discovered a bug in the central core of Linux; it would allow an attacker to acquire complete administrative control of any machine to which he had physical access.[14] You might call that a success for open source, except that the bug had been hiding in plain sight for at least eight years.

Why, then, is there so much more malware running on Windows than on Linux? Almost certainly for the same reason that there are more applications of every sort running on Windows than Linux. Like other application developers, malware authors want to reach the largest number of users with one piece of code. And the way to do that is to write your application for Windows.

It's a Password Problem. I used to take a lot of comfort from the fact that I didn't use just passwords for the things I most wanted to keep secure. I used a token. Every thirty seconds it displayed a different security code, known only to me and my home server. Even if a hacker could compromise my machine and record all my keystrokes, he couldn't know what the token was going to say next.

But this is the age of Twitter—and real-time hacking. For at least the last couple of years, criminals have been able to beat these token systems. Now, when the owner of a compromised machine starts typing in his temporary code, the malware phones home immediately. As

the owner types, each digit is sent to the hacker, who simply logs in with him.[15]

Really Important Transactions Can Be Confirmed Offline. If you're really worried, you may have locked down your financial accounts, so no money can leave the institution without a call to verify the transaction. In fact, even if you haven't locked everything down, you may get a call. Like the credit card companies, mutual funds and financial institutions have stopped trusting their customers' computers. For risky transactions, they insist on offline, or out-of-band, confirmation.

Out-of-band communication is today's most common fail-safe solution for computer compromises. To restore control of his Facebook account, for example, Bryan Rutberg had to send Facebook a separate, out-of-band message from a separate account.

But using another line of communication won't solve the problem for long. Hackers have already begun to build blocking programs into their malware. The programs prevent users from getting to Web sites that might detect and cure their infections. In the future, these programs may be able to thwart other efforts to cure an attack—diverting emails, for example, or corrupting the user's attempts to log on to hijacked sites.

The banks' offline solution is also at risk. Finding a truly offline method of communication is going to get harder. Businesses and consumers are switching in large numbers to "voice over IP," or VoIP, telephony. They cannot resist the allure of bringing to voice communications the cheap, flexible features of Internet communications. They cannot resist going just a little faster on the bike.

But the switch means that they are also bringing to voice communications all the insecurity that plagues other Internet communications. This raises the prospect of a whole new set of attacks, from "voice spam" and fraudulent telephone calls to the theft of incoming and outgoing phone calls. If an attacker who has compromised your computer's online bank account is also able to appropriate your Internet telephone, then it will be easy for the attacker to answer the phone when the bank calls—and to confirm that you really do want

to transfer your life savings to Spain or Nigeria. At that point, it will be cold comfort that switching to VoIP cut your monthly phone bill from $40 to $10 or even to $0.

The Military Has Solved the Problem With Classified Networks. The government used to have its own illusions about security. Maybe our unclassified networks are compromised, Defense Department officials used to say, but the *classified* networks are still bombproof. They can't be compromised by all this malware floating around the Internet. Because they aren't connected to the Internet. There's an "air gap" between the two.

That assumes, of course, that network security decrees are perfectly enforced—and that the most important secrets are only discussed on classified networks—notions that contradict everything we know about human nature.

But never mind, because the air gap illusion, too, has fallen prey to the exponential empowerment of hackers that we've seen in recent years.

The French navy's Rafale Marine jets train out of Villacoublay air base, in the southwest suburbs of Paris. These fighters are state of the art, packed with stealth and electronic warfare capabilities and capable of landing on carriers. But to do that, they first have to take off. And for two days in January, the jets couldn't take off. They'd been grounded by a hacker.[16]

The "Conficker" computer worm had been exploiting vulnerabilities in Windows servers for months. It was the most ambitious computer infection in years. At the time it had infiltrated as many as 15 million machines around the world. One of the ways it spreads is by infecting the USB thumb drives that carry data from one machine to the next. Even classified or isolated networks could be captured if a bad thumb drive was used to transfer data to a machine on a secured network.

That's what grounded the French fighters. Before the navy even knew it was under attack, the worm was coursing through its internal network. Rushing to contain the damage, the navy told its staff not to

turn on their machines, and its systems administrators began quarantining parts of the network. Too late for Villacoublay. Its systems were already hosed.

The Rafale fighter downloads its flight plans, a far more efficient process than paper-based systems. But once the contagion had spread to Villacoublay no flight plans could be downloaded. Until an alternative method of delivering the flight plans could be cobbled together, the Rafales were no more useful than scrap iron.

The French press reported the embarrassment in detail. Perhaps as consolation, it was careful to note that things could have been worse—and were, in Great Britain. There, the press said, twenty-four Royal Air Force bases and three-quarters of the Royal Navy Fleet had succumbed to Conficker.

The British and French navies may have been unintended victims of a worm designed for criminal ends. But after Conficker, no one can believe that an air gap is a security fail-safe.

They're Not Looking for Me. The last of the illusions, or at least the last of mine, is that I'm just not that interesting. Other people have more money. Other people have more valuable secrets. Who's going to come looking for me?

That's the last hope of every herd animal. The predators can't eat everyone. If you lie low and blend in, they won't pick you.

Wrong on two counts, I'm afraid. First, take this test. Add up your savings, car value, house equity, and investments. Is the total over $65,000? If so, you've got a lot of company on the globe. Probably 10 percent of the world's 6.8 billion people have assets exceeding that amount—say 700 million in all. Being one in 700 million sounds like pretty good herd-animal odds until you realize that, for every person with more than $65,000, there are nine people with less.

As computers become exponentially cheaper, most of those nine people will be able to get online. Then there will be nine people looking for ways to take money from you. And another nine for your spouse, nine for your neighbor, and nine for each of your business partners. Maybe nine each for every person you know.

So they *can* eat everyone.

There are already Nigerian hip-hop anthems and videos celebrating the rolling-in-money "Yahoozees" who fleece Americans like Howard Crank. The world is already full of scam artists willing to work for less than minimum wage. Most of them know English and have access to the Internet.

The relentless march of empowerment will soon give the Yahoozees of the Third World new tools for finding you. In a way, that's what a Spanish lottery email does. Most of us delete lottery spam. But if one in ten thousand responds, even with great caution, that person has selected himself for fleecing, and the pitch can then be tailored precisely to his failings. So what if that part of the scam is a bit labor intensive? There are nine people with nothing better to do than sit around trying to get into the mark's head.

Remember that real-time password-stealing program? Well, the thieves don't have to go looking for rich people to infect. Instead, they infect everyone, and let the malware find the rich ones. The password-stealing program consumes an infinitesimal part of a modern chip's processing power to run quietly in the background, watching and waiting until its victim logs on to one of about fifteen hundred predetermined financial sites. Anyone logging in to one of those sites, the authors figure, probably has enough money to be worth cleaning out. So when an infected computer sets itself apart from the crowd by logging on to a financial site, the malware alerts its author, who can now focus on taking money from that computer's owner.

Moore's Law has taken a lot of the work out of the hunt. And, thanks to the empowerment of information technology, it will keep making the job exponentially easier, year in and year out.

Until the predators find you, too.

You might think that's the worst of it.

But it's not, quite. It's not just that you could lose your life savings. Your country could lose its next war. And not just the way we're used to losing—where we get tired of being unpopular in some

Third-World country and go home. I mean *losing* losing: attacked at home and forced to give up cherished principles or loyal allies to save ourselves.

Plenty of countries are enthusiastic about using hackers' tools as weapons of war. At the start of a 2008 shooting war between Georgia and Russia over South Ossetia, for example, numerous Georgian websites were swamped by "denial of service" attacks. Security researchers found evidence that the attacks were coordinated and organized by Russian intelligence agencies. The year before, Estonian government agencies and banks were also crippled by denial of service attacks after the Estonian government moved a World War II memorial that had become a symbol of Soviet colonial rule. Estonia's foreign minister charged that the Russian government was behind the attacks. Russia denied the allegation. NATO, and European investigators were unable to refute their denial.

China has also been accused publicly of audacious computer attacks. German Chancellor Angela Merkel discovered that her office computers had been compromised in an attack blamed on the People's Liberation Army. India, France, and Taiwan have also suffered intrusions and attacks attributed to China. The compromise of the Dalai Lama's network was also widely blamed on China, as were a series of serious attacks on Google and other large U.S. companies in 2010. Like Russia, China has consistently denied all charges.

As I said before, in a strategic sense, the denials don't really matter. If the attacks weren't carried out by Russian and Chinese government agencies, that just means that there are more organizations and countries with effective cyberintelligence and cyberwarfare capabilities than we thought. And, in fact, five or ten years from now, there will be. That's because cyberattacks don't require heavy capital investments, the way nuclear weapons or stealth fighter jets do. Any nation willing to put ten of its best computer experts to work on a cyberintelligence program could probably have one in a year or two. (The Conficker worm that brought down British and French military systems could easily have been written by a single well-trained person.) Many

cyberattacks are simply a matter of individual effort. Put enough smart people on enough targets, and some of them will get through.

And that's why attacks on computer networks pose such a strategic threat to the United States in particular. We are an important intelligence target for practically every nation on earth. And attacking our networks is nearly risk-free; the list of suspects is about as long as the UN membership roster. In fact, there are incentives for them to help each other break into our networks. ("I've seized control of an email server at USDA, but what I really want is USTR's (Office of the U.S. Trade Representative). Want to trade? I could throw in the Commerce secretary's password to balance the deal.")

If you're a foreign government, breaking into U.S. networks is a twofer. You can start by stealing secrets. But if push comes to shove, you can use your access to destroy the same systems you've been exploiting. Corrupt the backup files, then bring the whole system down. Or start randomly changing data and emails until no one can trust anything in the system.

It wouldn't take much to create chaos. The financial crisis of 2008 became a panic when bankers began to disbelieve each other. No one trusted the other guy's books, so they stopped lending, and the world crashed. Could that same mistrust be created by modifying or destroying a few firms' computer accounting and trading records? We probably don't want to find out.

It's no secret how to fight a war against the United States. Slow us down, then cause us pain at home and wait for antiwar sentiment to grow. Cyberattacks are ideal for that strategy. Everything in the country, from flight plans and phone calls to pipelines and traffic lights, is controlled by networks susceptible to attack. A determined, state-sponsored attacker could bring them all down—and blame it on some hacker liberation front so we wouldn't even know whom to bomb.

The Pentagon has heard fifty years of warnings about not fighting land wars in Asia, where hand-to-hand fighting and sheer numbers can overwhelm an American army's technological edge. But now it turns out we've opened an electronic bridge, not just to Asia but to

the rest of the world, and now we're trying to defend ourselves hand to hand against all comers. It's hard to see how that ends well.

So that's the nub of the problem. No law of nature says that the good guys will win in the end, or even that the benefits of a new technology will always outweigh the harm it causes.

The exponential growth of information technology has made the Pentagon far more efficient at fighting wars; it has made our economy far more productive.

So far, it's been very good to us as a nation.

But it was good to Howard Crank, too, for a while.

The Hoover Institution on War, Revolution and Peace, founded at Stanford University in 1919 by Herbert Hoover, who went on to become the thirty-first president of the United States, is an interdisciplinary research center for advanced study on domestic and international affairs. The views expressed in its publications are entirely those of the authors and do not necessarily reflect the views of the staff, officers, or Board of Overseers of the Hoover Institution.

www.hoover.org

Hoover Institution Press Publication No. 591

Hoover Institution at Leland Stanford Junior University,
Stanford, California, 94305–6010

First printing 2010
16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

Manufactured in the United States of America

The paper used in this publication meets the minimum Requirements of the American National Standard for Information Sciences—Permanence of Paper for Printed Library Materials, ANSI/NISO Z39.48-1992. ♾

Cataloging-in-Publication Data is available from the Library of Congress.
ISBN-13: 978-0-8179-1154-6 (cloth)

ISBN-13: 978-0-8179-1156-0 (e-book)