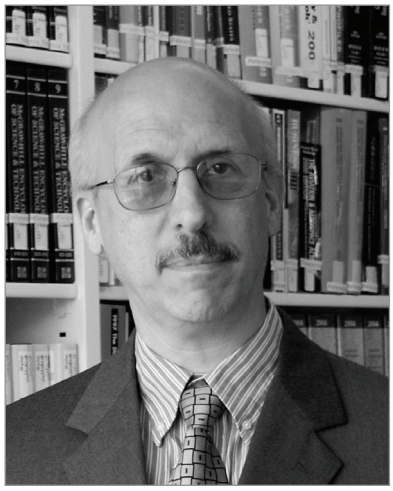
Is There a Cybersecurity Dilemma?[1]

Dr. Martin C. Libicki

A security dilemma is said to exist when one country cannot make itself more secure without making another less secure.[2] Circa 1913, for instance, if a major European country sought security by drafting more men, its neighbors would feel impelled to do likewise to recover their former levels of security. During the Cold War, when deterrence was the only feasible response to threat posed by the other side's nuclear weapons, any attempt to build more weapons or bring them to a higher state of readiness (for retaliatory purposes only, it would be claimed) would alarm the other side who would feel impelled to do likewise.

Is the same true in cyberspace? Might one country's attempt to increase its cybersecurity come at the expense of the cybersecurity *perceived* by potential adversaries?

In answering this question, two qualifications merit consideration. *First,* cybersecurity —efforts to prevent systems from being compromised—is useful against multiple threats. Some threats are purely criminal. Others are espionage, often but not always state-sponsored. Yet others are potentially disruptive or destructive, again often but not always state-sponsored. Although, it is possible to make a fair guess regarding the cost of cybercrime, the cost of espionage is conjectural (much depends on how purloined information is later used), and the losses from disruptive or destructive effects relatively low in much the same way that the costs associated with the destruction from nuclear war is currently zero. But the latter cannot be ignored, inasmuch as security is measured in terms of a contingent future, which may very well feature destructive cyberattacks among countries at war. *Second,* one must distinguish between whether one country's cybersecurity will, *in and of itself,* increase or decrease another country's cybersecurity, and whether a *particular action* to increase one country's cybersecurity will increase or decrease another country's cybersecurity. For instance, one country's



Martin Libicki (Ph.D., U.C. Berkeley 1978) has been a Distinguished Visiting Professor at the U.S. Naval Academy and a Senior Management Scientist at RAND since 1998, focusing on the impacts of information technology on domestic and national security. In addition he is a Distinguished Visiting Professor at the U.S. Naval Academy and has been an adjunct at Columbia University and Georgetown University. He wrote two commercially published books, Conquest in Cyberspace: National Security and Information Warfare, and Information Technology Standards: Quest for the Common Byte and has a textbook (Cyberspace in War and Peace) at the publisher's (U.S. Naval Institute Press). He is also the author of numerous RAND monographs, notably *Defender's Dilemma, Brandishing Cyberattack Capabilities,* and *Crisis and Escalation in Cyberspace*. Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO.

eliminating its own botnets will increase its own and everyone else's cybersecurity. However, one country's adopting particular active defense measures (such as intervening in another country's network to look for malware about to be deployed) may increase its own cybersecurity and decrease others'.

We now address the question in two parts: economics and international relations.

An Economics Perspective

When discussing whether one party's activities make another worse off, economists like to talk about externalities. They can be negative or positive. A negative externality, for instance, is created when my neighbor's smoke gets into my lungs. A positive externality is created when my neighbor's well-tended garden improves the view from my kitchen window. Correspondingly, if my cybersecurity activities make your networks less secure, then I am creating negative externalities; such activities should be discouraged (e.g., by taxing them) accordingly. If, conversely, my activities make you more secure, then I am creating positive externalities and they should be encouraged (e.g., by subsidizing them).

Positive externalities from improving cybersecurity are many and various.

One of the more oft-cited examples deals with bots. If I fail to keep my computer up to date with security patches, or if I practice less-than-perfectly-safe web surfing or e-mail practices, then my personal computer could be compromised. Many, perhaps most, of these compromised computers will become a bot, that is, a machine capable of being commanded to spam this or that site. Typically, thousands or millions of such bots are shepherded into botnets. Botnets, in turn, can be used to mount distributed

denial of service (DDOS) attacks to stifle access to parts of the Internet. Motives for DDOS attacks range from personal and political (Iranian attacks on US banks [3]) to criminal (pay us or we will shut down your gambling site just when wagers are being made). Many regard the DDOS potential arising from home users failing to maintain their machine's cybersecurity as so serious that they advocate allowing, or even mandating, Internet Service Providers to shut access to customers whose machines have been turned into bots. [4] It is unclear how such a policy might work in the coming future when most such machines are Internet-connected devices (e.g., thermostats, children's toys) whose owners are unaware that they are even networked.

A more direct version of herd immunity arises in the way viruses and worms can spread from one machine to another. The cleaner my machine is, the more likely it can ward off infection, and hence, less likely that it will infect you. The Internet was convulsed with a series of rapidly-spreading worms, starting with Code Red in 2001, and continuing on through NIMDA, MSBlast, SoBig, MyDoom, Slammer, and Witty among others. But a patch to Microsoft XP (Service Pack 2) released in August, 2004 essentially eliminated that particular threat. Although replicating malware exists—indeed, hackers rely on malware with such properties to move laterally within an organization—its spread is generally limited to machines that use common services (e.g., printers, file shares), and, hence, rarely leaves the confines of organizations. They do not spread globally within hours as the earlier versions did.

A security dilemma is said to exist when one country cannot make itself more secure without making another less secure.

There are also general forces that promote herd immunity in cyberspace. The greater the percentage of ill-secured machines connected to the Internet, the greater the potential rewards for cyber-criminals. Not only is there a larger target set, but the odds of turning a random machine are higher; both offer more reward per unit of effort. The greater the rewards for criminality, the greater the investment that criminals will make in improving their capabilities. The same logic works for providers of cybersecurity services. The more diligently users—notably, organizations with complex networks—attend to cybersecurity the larger the market they create for such providers ($75 billion a year in sales and growing [5]), and the greater the incentive for start-ups (of which there are thousands) to invent better mouse-traps. Again, my greater diligence means more and better products for you to use. Even if individuals rarely buy such merchandise themselves, they show up in products people use, such as web browsers. Finally, the more secure an infrastructure is, particularly against data theft, the more people can engage in electronic commerce without undue worry—and that also benefits all.

Conversely, those who remember the joke that ends, "I don't have to outrun the bear, I just have to outrun you," might counter that if it is too easy for criminals to prey on certain users, they may not have to improve their arts to make money. Thus, they would leave the more fastidious users alone, and turn their attention to the less fastidious. If so, one person's sloppiness gives them an easy target, and increases the odds that they can satisfy themselves without working hard to attack another person. The difficulty in predicting as much beforehand arises from trying to understand what role signaling plays in the relationship between one person's cybersecurity and another's. Hackers may have little *a priori* knowledge of who is or is not an easy target. In 2015, a spokesman for a cybersecurity startup made the claim that an APT attack was not only thwarted, but discouraged from continuing to batter an organization that had purchased one of the startup's products after the product was discovered working on a target server.[6] Consider piracy as an analog. The more treasure ships that roam the high seas, the more opportunities for pirates, the greater the incentive to become one. Conversely, the more treasure ships that roam the seas, the less likely the existing crews of pirates will pick on mine. Now assume that some of these treasure ships are armed enough to imperil pirate ships. Once this is so, piracy carries grave risks. If pirates cannot determine which ships are armed before confronting one, then they will hesitate to attack any ship. The benefits from some being armed accrue to all ships. However, armed ships might want to advertise that fact because it helps them avoid confrontations in the first place, which is preferable (unless they have been armed by, say, a government for the express purpose of eradicating the pirate menace) to enduring the damage and casualties of winning a confrontation. Unless unarmed ships can appear to be armed, they are scarcely better off for there being armed ships. In that case, there are no positive externalities.

The greater the percentage of ill-secured machines connected to the Internet, the greater the potential rewards for cyber-criminals.

The closest analogy to ship signaling here may be information sharing, which is an unquestionably good thing (irrespective of the merits of any one piece of legislation to foster information sharing). Two forms of information sharing merit note: general and specific. General benefits occur when organizations share among themselves stories of how their own failures and bad choices allowed them to be hacked. As in aeronautical engineering or medicine, knowledge (and safety) advances one bad outcome at a time—as long as these outcomes are shared and dissected for lessons learned. The more people who share, the more examples are shared, and the faster the knowledge base grows (even as hackers, themselves, share information), and thus the greater the skill base for repelling hackers. Specific benefits occur when organizations share information about specific

hackers (e.g., Unit 61398 identified by the Mandiant Corporation [7]) who have a particular repertoire of malware, social engineering tricks, or the like. Such knowledge allows organizations, notably those with sophisticated firewalls or intrusion detection systems, to use the signatures generated by this information to block intrusions. Conceivably, telltale signs of compromise may be shared to detect and eradicate infections that have already taken root in an organization's networks. If the global cyber community gets to the point where such information can be routinely shared, the odds of a sufficiently broad attack (where the same indicators can be found over large numbers of different organizations) can become vanishingly small even if individual system compromises can remain undiscovered for long periods of time (these days, the average APT attack goes unnoticed for an average of seven months [8]).

The more secure an infrastructure is, particularly against data theft, the more people can engage in electronic commerce without undue worry—and that also benefits all.

There is a broader lesson here about incentives and institutions. The neoclassical market beloved by economists is built around a model of large numbers of small decision-makers whose decisions might produce externalities. Incentives are manipulated so that positive externalities are encouraged and negatives ones discouraged. But the world of cybersecurity is one of institutions. Rapidly replicating worms did not stop because users were penalized for being sloppy, but because one organization (Microsoft) altered its product to disable such worms. Information sharing will only begin to benefit cybersecurity after institutions arise that find systematic ways of converting information into knowledge and practice.

An International Relations Perspective

The problem, viewed from an international relations perspective, assumes an anarchic world in which countries do, in fact, threaten one another in cyberspace. Such threats could be used to support conventional kinetic capabilities: e.g., if I can disable your anti-aircraft weapons, my threat to bomb you would have greater credibility. They can also be used independently of armed conflict: if you intervene in my back yard, I will create chaos in your banking system.

To address whether one nation can increase its cybersecurity without another nation's cybersecurity being reduced requires some context. For many forms of combat, the same weapon can be used for offensive and defensive purposes. If a country fears a million infantry on its border (*circa* WWI) its most basic military response is to raise a million infantry on its own borders; it could announce that its infantry's purpose was defensive,

but no one could assume that such forces could not go on the offense. With nuclear weapons in the Cold War, nothing was defensive. The doctrine of deterrence would not have been so compelling had satisfactory defenses been available.

But while the security dilemma is harder to avoid if all defensive weapons were, at the same time, potentially offensive, the dilemma does not disappear if there were truly defensive weapons. *Circa* WWI, forts on the Western Front were defensive weapons; after all, they sat in a country's own territory. But the other side could argue that nothing was as offensive as a good defense because it permitted one side to attack with reduced risk. Their forts would limit the risk of failure by allowing a much smaller force to stay back and defend the territory against unexpected reverses or occasional enemy break-outs. Although US (conventionally-armed) anti-ballistic missiles (ABMs) were totally defensive, they frightened the Soviet strategists who believed the United States, so protected, could launch a first strike without fear of repercussions. Cybersecurity works the same way; *most* of what brings about cybersecurity (e.g., better computer hygiene) cannot possibly make others less secure *directly*—but could conceivably make others less secure *indirectly* by encouraging cyberattacks by those who convince themselves that their own cybersecurity makes them invulnerable to retaliation.

Central to this logic was that when discussing WWI ground forces, or Cold War era nuclear weapons, countries were at the top of their escalation ladder. It is not as if someone could trump these force elements with other unused weapons at their disposal. Cyberattacks, of course, can be trumped—certainly by nuclear weapons, and almost as certainly by strategic bombing and conventional land operations. It is difficult to imagine that the costs of a strategic cyberattack campaign would exceed that of even a small war, particularly if cost and coercion are measured in terms of human casualties; after all, no one has died yet as a direct result of a cyberattack. Thus, the degree of insecurity in one country that may arise from the fact that their enemy's society enjoys cybersecurity is limited to the pain that it is willing to take without escalating to physical force. This pain is not zero because there are good reasons not to let a fight in cyberspace bleed over into the physical world—but it *is* limited.

But does that mean that greater cybersecurity in one country will always reduce the security of another? Not directly, in most cases. To begin with, almost all defensive actions in cyberspace are unmistakably defensive: examples include measures such as diligent patch management and least privilege, multi-factor authentication, and intrusion detection systems. They cannot be used to break into systems, in large part, because such actions take place within the computer networks being defended (aka *blue space*).

But there are exceptions, many of which fall under the rubric of active defense. If President Obama's speech defending his management of the NSA is any indication, offensive capabilities are a vital part of cybersecurity defense.[9] It is easy to imagine how poking around in the attacker's networks—*red space*—might provide indications and

warning of a cyberattack, just as it might reveal indications and warnings of plans to use physical force. Private organizations routinely crack servers, many of them belonging to third parties—*gray space*—looking for evidence that their own stolen files are sitting there; in doing so they collect information that allows the tracks of attackers to be found in the systems they are defending. Other defenses have been known to disable the computers from which attacks are coming from (one from the late 1990s caused the attacker's computer to keep throwing up new windows onto the screen). There was even a case in which the defender left a corrupted file out for the attacker to grab and open, which then infected the attacker's machine, and took a screen shot of the perpetrator.[10] These are instances where the ability to defend relies on the ability to attack—and, in many cases, the victims of such attacks are not only systems owned by the original attacker, but any system in the attacking country.

Information sharing will only begin to benefit cybersecurity after institutions arise that find systematic ways of converting information into knowledge and practice.

But how much concern should be associated with these techniques before concluding that what brings me cybersecurity brings you cyberinsecurity? Most of these offensive defenses can be warded off by attackers who anticipate that they themselves may be attacked. For instance, when electronic intelligence collection is a problem, isolation provides much of the solution (for those operations that require access to the outside world, hackers could, for instance, use a computer and an IP address once, and then move on). When there are prospects that code in one's repositories could get altered before being delivered, digital signatures can assure authenticity. Obfuscation and encryption techniques can inhibit what others can collect from intermediate servers in gray space. And all the techniques that rely on returning poisoned materials to the attacker can either be filtered out (e.g., by accepting only pre-selected inputs) or can be transferred to an isolated computer for the latter to process (*that* computer may be infected but it cannot be controlled by the target because of its isolation). These techniques are not free, and some (such as filtering) require some sophistication, but if cyberwar is serious, then these active defense techniques are hardly speed bumps, much less barriers.

If there is a clean separation between defensive and offensive techniques, then the cybersecurity dilemma therefore has to be indirect: my improved cybersecurity emboldens me to attack your systems. The major impediment to this formulation is whether confidence in one's own security is merited. Alternatively, my cybersecurity will reduce your confidence in prevailing in a confrontation, and therefore you will yield even at the expense of your *broader* security goals; here the issue is the other side's confidence in *your* cybersecurity.

But can aggressors legitimately feel that their systems are impenetrable or even sufficiently well protected to the point where they can convince themselves that their losses from cyberattack are manageable regardless of what their foes might do? Consider the first clause. North Korea may be impenetrable (although even they are becoming gradually more connected), but only because North Korea has crippled its own economy in the service of *juche* (roughly: self-reliance). Yet most normal countries are increasingly dependent on information systems and growing more so by the day. As a general rule, any Internet-exposed system built on personal computers cannot be protected reliably against an even-halfway sophisticated opponent absent enormous expenditures on cybersecurity.[11] Only a fool can be confident that having traced out all possible attack vectors and having figured out how to block them, conclude that it was perfectly secure. Not only are systems become far too complicated to know all possible attack vectors, but there is very little software that lacks (zero-day) vulnerabilities. And this does not include other sources of non-technical vulnerabilities such as suborned insiders or sloppy users. True, our computers are far more vulnerable than they need to be—Apple's iOS operating system, because of its closed nature is two orders of magnitude safer than PC operating systems (even though MacOS is no more secure than Microsoft Windows). And machines whose every instruction is burned into hardware cannot host malware once they have been turned off and back on. Nevertheless, even a world without malware is not a perfectly secure world because complex software is heir to unwanted results (e.g., a deliberately malformed database query can often persuade databases to spill their contents unexpectedly), and because authentication and authorization is still an art not a science.

If it is hard for an aggressor to feel deservedly confident in its invulnerability to counterattack, the other side might not necessarily feel as if its own efforts to penetrate adversary systems are futile. This works both ways. The aggressor may know what investments it has made to ensure its cybersecurity, but if the other side is testing the aggressor's defenses by trying to compromise its systems, it may know more than the aggressor about how far it was able to get. What attackers may not know is what the effects of its cyberattack successes might be on its target's ability to get work done (for instance, the target may have secret back-up capabilities), or its ability to recover quickly from having been attacked.

In practice, rational aggressors are going to look at a vast tableau of capabilities, both offensive and defensive, when making threats or carrying them out. The more confidence they have in their cybersecurity the bolder they are likely to be, but there are so many assumptions packed into the cybersecurity relationship; enhancing actions, actual cybersecurity and perceived cybersecurity on the one hand, and the relationship of cybersecurity to overall *defensive* capabilities *plus* the relationship of defensive capabilities to the ability to take to the offense, that the gearing between investing in cybersecurity, and posing a threat to neighbors may be vanishingly small. It is worth remembering that cybersecurity has uses beyond simply warding off attacks from

enemy countries: other reasons include attacks from insiders, spies from every imaginable country, whoever is calling themselves *Anonymous* this week, and even the run of disasters, accidents, and bad software (improving resilience, for instance, preserves a system's capabilities against threats from human error, acts of nature, and bad software).

Another facet of cybersecurity which dulls the security dilemma is the difficulty one side has in knowing what the other side is doing to secure its networks. In 1914, when one country mobilized, its foes were persuaded to do likewise for fear of falling behind in the coming conflict, and despite some desultory attempts (largely, by Russia) to hide the fact of mobilization, few were fooled. In the nuclear context, putting forces on alert in response to a crisis exacerbated a crisis in the mind of the other, since the only logical response to a nuclear threat in a world of deterrence was to increase the threat that one could reciprocate to an adversary.

Rational aggressors are going to look at a vast tableau of capabilities, both offensive and defensive, when making threats or carrying them out.

One of the factors favoring stability in cyberspace—counterintuitively for a medium in which everything supposedly works at the speed of light—is that it is difficult to detect quickly when the other side is advancing its capabilities. Cyberwar is usually an activity whose tools are deeply hidden (because if one knew how attack tools worked, defeating them would be a straightforward matter of fixing or routing around the vulnerabilities they exploited). If one goes by what attackers have actually done, there is a lag (measured in weeks and months) between the decision to attack a target, and its successful penetration and then (notably for espionage and subtle corruption) there can be an additional lag between the action and its detection. It can also be difficult to react *defensively* to the other side's quick improvements. Even if patches can be installed, literally, within minutes, the more fundamental changes in computer code and network architecture (e.g., restricting access privileges, adjusting input filters) take time to create and test. On the offensive side, the key to increased capability is not more weapons (it is trivially easy to replicate malware), but better weapons, notably those that work against hitherto, undetected vulnerabilities. The latter can take time, often an unpredictable time, to develop.

The cybersecurity dilemma fades further when countries start depending on the same infrastructure for their cybersecurity. In one sense they already do: commercial software is a global commodity, and cybersecurity firms take customers from anywhere. Vulnerabilities for one are vulnerabilities for all; patches for one are patches for all. If and as cloud computing spreads, various countries may find themselves dependent on the security of the same providers. It will be interesting to see how moves towards autarky in cyberspace

(notably by Russia, itself following the lead of Iran and North Korea) affect such trends.

Finally, cybersecurity is useful against both espionage and attack. Increasing cybersecurity in one country may make it difficult for another country to collect intelligence on it (or not: it may take an unaffordable level of cybersecurity to keep a really professional espionage agency from collecting most of what it needs from Internet-connected networks). The failure to collect intelligence may lead to insecurity; note how vociferously the FBI and NSA criticize the access to hard-to-break encryption technologies that they claim terrorists now enjoy.

The Calculus of Insecurity

Ultimately, any security dilemma is about the relationship between two countries. If both live in a zero-sum world in which it is not stability and security that both sides seek, but power vis-à-vis the other, then, everything touches the security dilemma because nothing will make both sides more powerful *vis-à-vis* the other. But this condition is rare. Even dedicated mutual enemies such as ISIL and the United States can have common objectives (e.g., changing the Syrian regime; limiting Iranian influence).

More commonly, every country has a mixed relationship with every other country. Russia and the United States may view each other with suspicion regarding former Soviet countries (e.g., Ukraine), but both of them have criminals as common enemies. Cybersecurity that protects systems from being compromised by criminals is largely the same cybersecurity that protects systems from being compromised by anyone else, notably other countries. If a country improves its cybersecurity by catching criminals, there will be fewer criminals; thus the other country is better off. If countries care about preventing crime more than they worry about each other, they share a mutual interest in improving cybersecurity.

Last, it helps to remember that security is not just the feeling that one can withstand an adversary's attacks, but also the feeling that an adversary is unlikely to try. This introduces a paradox that affects all forms of warfare: countries may be motivated to start trouble not only because they are fearless but fearful (and believe that it must act before falling irretrievably behind). Similarly, they may overreact to events because they are twitchy and believe that the failure to act will leave them exposed to surprise attack. Both factors were in play to start WWI. Germany was concerned with a rising Russia, and all sides feared being out-mobilized by potential foes.

In cyberspace, ambiguity can make such fears take a malign form. It is difficult to tell who is attacking whom in cyberspace (and for some attacks, it is often difficult to know, even afterwards, what information was taken or what processes were corrupted). Distinguishing cyber-espionage from an impending cyberattack when a hostile implant (inserted back door) is found is difficult because one implant can be used to do both.

Cyberwarriors may believe (notwithstanding the lack of corroborating facts) that they can pre-empt planned cyberattacks by carrying out cyberattacks on potential attackers. In the fog of misperception, a nervous country may be apt to assume the worst and lash out to protect itself; by so doing it may start a fight that a more secure country might have avoided.

In the end, the major policy question is whether to enable or disable cyberwar for everyone by promoting a global culture of cybersecurity and waging incessant war on vulnerabilities and ignorance. Those who think that the United States is currently in a no-holds-barred contest with other major powers may think such efforts naïve. Others who think that cyberwar provides a chance for countries to contest without serious consequences—when alternative forms of contestation may kill people—may think such efforts counterproductive. But those who think that creating new forms of conflict generally detracts from everyone's ability to get along may want to give the matter serious thought. In the end, there is less of a cybersecurity dilemma than it seems.

The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

NOTES

1. See for instance, Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics,* 30, 2, (January 1978), 167-214.

2. Nicole Perloth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *New York Times,* January 8, 2013; http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

3. Something similar has been used in Australia; see Sean Gallagher, "Is an ISP code of conduct the best way to fight botnets?," *Ars Technica,* September 22, 2011, http://arstechnica.com/business/2011/09/us-government-looks-to-fight-botnets-with-isp-code-of-conduct/.

4. "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015," September 23, 2015; http://www.gartner.com/newsroom/id/3135617.

5. Andrea Shalal, "U.S. firm CrowdStrike claims success in deterring Chinese hackers," *Web Culture,* April 14, 2015, http://www.webculture.com/17/Tech%20Top%20News/16/a/19280884/US_firm_CrowdStrike_claims_success_in_deterring_Chinese_hackers.

6. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (report, 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

7. Statement for the Record by Richard Bejtlich Chief Security Strategist FireEye, Inc. Before the U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations Understanding the Cyber Threat and Implications for the 21st Century Economy, March 3, 2015; http://docs.house.gov/meetings/IF/IF02/20150303/103079/HHRG-114-IF02-Wstate-BejtlichR-20150303.pdf.

8. We cannot prevent ... cyberthreats without some capability to penetrate digital communications, whether it's to ... intercept malware that targets a stock exchange, to make sure air traffic control systems are not compromised or to ensure that hackers do not empty your bank accounts. From "Transcript of President Obama's Jan. 17 speech on NSA reforms," *Washington Post,* January 17, 2014, http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

9. Charlies Osborne, "Georgia turns the tables on Russian hacker," *ZDNet,* October 30, 2012, http://www.zdnet.com/georgia-turns-the-tables-on-russian-hacker-7000006611/. The target planted malware in a file that the hacker took. The hacker's computer was infected when the file was opened. The computer's webcam then turned on and photographed the presumed hacker.

10. *Circa* 2014, JPMorgan Chase's annual expenditures of $250 million a year did not prevent their systems from being hacked (although they may have prevented the hack from having consequences more serious than the release of information normally found in phone books); see Jessica Silver-Greenberg, Matthew Goldstein, and Nicole Perloth, "JPMorgan Chase Hacking Affects 76 Million Households," October 2, 2014; http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/.