M McAfee®
An Intel Company

THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE

Center for Strategic and International Studies

July 2013

Report

CONTENTS

Introduction

Is cybercrime, cyber espionage, and other malicious cyber activities what some call "the greatest transfer of wealth in human history," or is it what others say is a "rounding error in a fourteen trillion dollar economy?"

The wide range of existing estimates of the annual loss—from a few billion dollars to hundreds of billions—reflects several difficulties. Companies conceal their losses and some are not aware of what has been taken. Intellectual property is hard to value. Some estimates relied on surveys, which provide very imprecise results unless carefully constructed. One common problem with cybersecurity surveys is that those who answer the questions "self-select," introducing a possible source of distortion into the results. Given the data collection problems, loss estimates are based on assumptions about scale and effect—change the assumption and you get very different results. These problems leave many estimates open to question.

The Components of Malicious Cyber Activity
In this initial report we start by asking what we should count in estimating losses from cybercrime and cyber espionage. We can break malicious cyber activity into six parts:
• The loss of intellectual property and business confidential information
• Cybercrime, which costs the world hundreds of millions of dollars every year
• The loss of sensitive business information, including possible stock market manipulation
• Opportunity costs, including service and employment disruptions, and reduced trust for online activities
• The additional cost of securing networks, insurance, and recovery from cyber attacks
• Reputational damage to the hacked company

Put these together and the cost of cybercrime and cyber espionage to the global economy is probably measured in the hundreds of billions of dollars. To put this in perspective, the World Bank says that global GDP was about $70 trillion in 2011. A $400 billion loss—the high end of the range of probable costs—would be a fraction of a percent of global income. But this begs several important questions about the full benefit to the acquirers and the damage to the victims from the cumulative effect of cybercrime and cyber espionage.

Using Analogy to Set the Bounds for the Cost of Malicious Cyber Activity
We use several analogies where costs have already been quantified to provide an idea of the scope of the problem, allowing us to set rough bounds—a ceiling and a floor—for the cost of malicious cyber activity, by comparing it to other kinds of crime and loss.

- **Car Crashes:** One way to think about the costs of malicious cyber activity is that people bear the cost of car crashes as a tradeoff for the convenience of automobiles; similarly they may bear the cost of cyber crime and espionage as a tradeoff for the benefits to business of information technology. The Center for Disease Control estimated the cost of car crashes in the US at $99 billion in 2010. The American Automobile Association estimated the 2010 cost of at $168 billion.

- **Piracy:** A weakly governed space exploited by criminals could describe some oceanic areas as well as the internet. The International Maritime Bureau estimated the annual cost of piracy as somewhere between $1 billion and $16 billion in 2005 (cyber is not the only field where estimation is difficult). To put these figures in context, the annual value of maritime trade in 2005 was $7.8 trillion, which means piracy costs equaled at most 0.02 percent of the total.[1]

- **Pilferage:** Companies accept rates of "pilferage" or "inventory shrinkage" as part of the cost of doing business. For retail companies in the US, this falls between 1.5% and 2.0% of annual sales—one 2008 estimate put pilferage losses at 1.7%. Using a "pilferage" approach that assumed the same rate of loss for malicious cyber activity would put the upper limit somewhere between 0.5% and 2% of national income. For the US, this would be $70 billion to $280 billion. A central problem for the "pilferage theory," however, is that many companies do not know the extent of their losses, leading them to make decisions about what is an acceptable loss based on inadequate information.

- **Crime and Drugs:** One frequently heard comparison is that malicious cyber activity is more lucrative than the drug trade. This begs the question of whether we know the drug trade's value. In 2012 the UN Office on Drugs and Crime estimated the cost of all transnational organized crime as $870 billion, or 1.2% of global GDP.[2] It estimated $600 billion of this figure came from illegal drug trafficking. If cyber losses also cost the same share of global GDP, the cost could be more than $600 billion.

What's the Harm?

If we are right in assuming that "tolerated costs" from malicious cyber activity falls into the same range as car crashes, pilferage, and drugs, this is a "ceiling" for an estimate of loss. They suggest that at most, cybercrime, cyber espionage costs less than 1% of GDP. For the US, for example, our best guess is that losses may reach $100 billion annually. To put this in perspective, annual expenditures on research and development in the US are $400 billion a year and $100 million in stolen IP does not translate into $100 million in gain for the acquirer.

One difficulty lies in quantifying the cost of damage to national security. The theft of military technology could make nations less secure by strengthening potential opponents or harming export markets in aerospace, advanced materials, or other high-tech products. There is a link between cyber espionage directed at commercial targets and cyber espionage targeted on military technology. It is often the same actors pursuing a collection plan that targets both military and commercial sources. Engaging in cyber espionage can improve cyber attack capabilities. We cannot accurately assess the dollar value of the loss in military technology but we can say that cyber espionage shifts the terms of engagement in favor of foreign competitors.

The effect of malicious cyber activities on jobs needs further work. The Commerce Department estimated in 2011 that $1 billion in exports equaled 5,080 jobs.[3] This means that the high end estimate of $100 billion in losses from cyber espionage would translate into 508,000 lost jobs. While this translates into a third of a percent decrease in employment, this is not the "net" loss as many workers will find other jobs. The real concern might be if the lost jobs are in manufacturing or other high paying sectors. If workers displaced by cyber espionage do not find jobs that pay as well or better, the victim country would be worse off. The effect of cyber espionage may be to move workers from high paying blue-collar jobs into lower paying work or unemployment.

1 http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG697.pdf

2 http://www.unodc.org/unodc/en/frontpage/2012/October/transnational-crime-proceeds-in-billions-victims-in-millions-says-unodc-chief.html

3 International Trade Administration, *Jobs Supported by Exports: An Update,* March 12, 2012, http://www.trade.gov/mas/ian/build/groups/public/@tg_ian/documents/webcontent/tg_ian_003639.pdf

Putting Malicious Cyber Activity in Context

CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

Next Steps for Estimation

Putting a number on the cost of cybercrime and cyber espionage is the headline, but the heart of the matter is the effect on trade, technology, and competitiveness. Answering these questions will help us put the problem in its strategic context. While the cost of cybercrime and cyber espionage to the global economy is likely billions of dollars every year, the dollar amount, large as it is likely to be, may not fully reflect damage to the global economy. Cyber espionage and crime may slow the pace of innovation, distort trade, and create social costs from job loss. This larger effect may be more important than any actual number and it is one we will focus on in our final report.

Crime Pays—But How Well?

Extracting value from the computers of unsuspecting companies and government agencies is a big business. The size of any loss, however, is the subject of intense dispute. Is this what one senior official called "the greatest transfer of wealth in human history," or is it what a leading economist called a "rounding error in a fourteen trillion dollar economy?"

Cyber crimes against banks and other financial institutions probably cost many hundreds of millions of dollars every year. Cyber theft of intellectual property and business-confidential information probably costs developed economies billions of dollars—how many billions is an open question. These losses could just be the cost of doing business or they could be a major new risk for companies and nations as these illicit acquisitions damage global economic competitiveness and undermine technological advantage.

Previous estimates of the annual losses to businesses from cyber espionage show a startling variation, ranging from few billion dollars to hundreds of billions. The wide range of estimates reflects the difficulty of collecting data. Companies conceal their losses and some are not aware of what has been taken. Intellectual property is hard to value in the abstract. Estimates are often based on anecdotes or surveys. These problems combine to leave some previous estimates open to question.

The cost of malicious cyber activity involves more than the loss of financial assets or intellectual property. There are opportunity costs, damage to brand and reputation, consumer losses from fraud, the opportunity costs of service disruptions "cleaning up" after cyber incidents, and the cost of increased spending on cybersecurity. Each of these categories must be approached carefully, but in combination, they help us gauge the cost to societies. In many cases we have used the United States as an example. This reflects, more than anything else, the fact that data is more readily available from US sources.

In an ideal world, aggregating the various factors would be straightforward. This is not possible. In all of the categories of malicious cyber activity, the data is incomplete. Data collection is complicated by definitional difficulties. Should cyber crime, for example, include all crimes committed using cyber means or only those crimes that could only be committed with cyber tools, leaving out crimes that would have otherwise been committed via traditional criminal means. One way to think about this is to ask, if there was no internet, would this crime have occurred?

Two important caveats shape this comprehensive view. First, we will try to estimate "net" loss, which is particularly important for estimating the effect of a temporary disruption of service. A store knocked offline for a day may lose $10,000, but if customers wait or go to another store, the net loss to the

Estimating the Cost of Cybercrime and Cyber Espionage

economy is much smaller. Second, we will try to use market values rather than a value assigned by the victim. A company may spend a billion on research, but it is the expected return on this research that determines its worth, not the expenditure.

A rough guess? Losses to the US (the country where data is most accessible) may reach $100 billion annually. The cost of cybercrime and cyber espionage to the global economy is some multiple of this likely measured in hundreds of billions of dollars. To put this in perspective, the World Bank says that global GDP was about $70 trillion in 2011. A $300 billion loss—and losses are probably in this range—would be four tenths of one percent of global income. But this seemingly trivial amount begs several important questions about the full benefit to the acquirers and the damage to the victims from the cumulative effect of continuous losses in cyberspace. This question of the effect and consequences of the loss is more important than any actual number and it is one we will focus on in this essay and in our final report.

We reviewed previous studies to develop our own understanding of the problem. For example, a 2010 estimate by a German corporate security association of Germany's losses of intellectual property put them at a minimum of perhaps $24 billion (most, but not all, from cyber espionage).[4] Since the US GDP is roughly five times that of Germany, a very

crude extrapolation would project the size of the German loss onto the larger American economy and put an upper bound for US losses at $120 billion.[5] Another report, widely criticized, put the cost to the UK at $27 billion.[6] These figures represented about 2% of the UK's GDP and would translate into about $280 billion for the US. Three quarters of these losses were ascribed to losses of intellectual property by companies, based on a series of projections and assumptions about IP valuation that others questioned.

Some previous estimates of the cost of cybercrime relied on surveys, which are notoriously imprecise unless very carefully constructed. Surveying a few companies or even a few hundred companies and then extrapolating costs from their responses is a dangerous methodology. There are significant differences among economic sectors in vulner-ability. There are rules for deciding on sample size and selection, but imperfect samples are a com-mon flaw in surveys. Many previous studies use a sample population that is too small for us to feel confident in the results. One common problem in cybersecurity surveys is that those who answer the questions "self-select" and we do not know if their experience is the same as those who chose not to respond. Companies that have concealed large losses, for example, might choose to not respond, introducing a possible source of distortion into the survey.

4 http://www.spiegel.de/international/world/0,1518,713478-6,00.html
5 http://www.dw-world.de/dw/article/0,,5645869,00.html;
  http://intelnews.org/tag/berthold-stoppelkamp/
6 Ref to Ross Anderson paper

The most important area for loss is in the theft of intellectual property and business confidential information—economic espionage

The Components of Malicious Cyber Activity

In this initial report we attempted to scope the problem and discuss what to count in estimating losses from cybercrime and cyber espionage. We looked at physical analogies—pilferage rates for example—to help us in measuring the loss from malicious cyber activities. We attempted to break malicious cyber activity into component parts. The aggregate of these parts would let us measure the total cost to societies of malicious cyber activities, but for each of the components of the cost of malicious cyber activities category, data is weak or nonexistent and any estimate must be approached with this limitation in mind. The components are:

• The loss of intellectual property.

• Direct financial loss from cybercrime.

• The loss of sensitive business information (such as negotiating strategies), including possible stock market manipulation.

• Opportunity costs, including service disruptions, reduced trust online, the spending required to restore any "lead" from military technology lost to hacking, and the realignment of economic activity as jobs flow out of "hacked' companies.

• The additional cost of securing networks and expenditures to recover from cyber attacks.

• Reputational damage to the hacked company.

Intellectual Property Losses

The most important area for loss is in the theft of intellectual property and business-confidential information—economic espionage. It is difficult, however, to precisely estimate the losses. This is in part because cyber spying is not a zero-sum game. Stolen information is not really gone. Spies can take a company's product plans, its research results, and its customer lists today, and the company will still have them tomorrow. The company may not even know that it no longer has control over that information.

There are many ways to determine the value of intellectual property. One is to estimate what it would fetch on the market if offered for sale or for licensing. Companies can value their intellectual property by determining the income streams it produces and is expected to produce in the future. Companies can also estimate what it would cost to replace intellectual property as a means of estimating its value, although a reliance on inputs for estimating value can be very misleading.[7] The actual value of intellectual property can be quite different from the research and development costs incurred in creating it. If a company spends a billion dollars on a product that fails in the market, and a foreign power steals the plans, the loss is not a billion dollars but zero—the invention's market value.[8]

7 CRS, The Economic Impact of Cyber-Attacks, April 1, 2004
8 http://www.wipo.int/sme/en/documents/value_ip_intangible_assets.htm

Extracting information from a computer network does not always mean there is immediate benefit to the acquirers. They may lack the advanced manufacturing capacity or skill needed to produce military or high tech products. For some advanced technologies, there may be a lag of five to ten years between the theft of the IP and when it appears as a competing product. This lag in the use of pilfered intellectual property complicates the estimation of loss from malicious cyber activity. The rate at which a competing product based on stolen intellectual property appears varies from sector to sector. Some take years. Others, such as high speed trains or wind power generators, appear rapidly. In some cases, acquirer of the technology has been able to put a product on the market before the victim can introduce their own, legitimate version.

One way to put these possible losses in context is to consider a US company with $1 billion in intellectual property, all of which is extracted by foreign hackers and given to a competitor. This competitor now has the advantage of access to valuable intellectual property for which it did not have to pay. However, if the competitor that illegally acquired the intellectual property is unable to develop a competing product, the theft does not create additional risk for the victim. To suffer loss,

the acquiring company would have to use the IP in a way that harms the victim, by offering a competing product or by improving their bottom line through reduced R&D costs.[9]

Making high tech products requires "know-how" as much as blockbuster IP—knowing how to run a manufacturing process, where to buy the cheapest inputs, which customers are most interested, what designs actually move product, etc. All of those things hold back companies that rely on cyber espionage. But if the company can ask each time they hit a roadblock, "How did the victim get over this barrier?" and then go back find the answer in the victim's files, then they can quickly acquire the practical know how to use the stolen IP.

Historically, state sponsored commercial espionage has focused on areas of great interest to governments, such as military and advanced technologies. More recently, some countries seem to use cyber espionage as a normal part of business. Cyber espionage by nation states to benefit their companies is a kind of state aid to those companies that is cheaper than traditional subsidies. This privatized espionage can be deployed against a much broader swath of companies. One interview with intelligence officials told of a US furniture company being hacked and losing its IP, only to see furniture made from its designs being offered online

9 http://www.chathamhouse.org/media/comment/view/177189

to wholesalers. There are similar stories involving efforts to use cyber techniques in attempts to acquire breakfast cereal recipes, running shoe designs, automobile part technologies, and soft drink formulas. These are not "strategic industries," but their losses from cyber espionage can still be significant.

The victim company still has access to the intellectual property. It has not lost the ability to make the product; what has in fact happened is that it now faces a new competitor. The risk of this competition is increased if the new foreign competitor has access to other government subsidies that allow it to sell at a lower price or if it is supported in its domestic market by barriers that hamper outside companies from competing. We need, in our assessment of the cost of cyber espionage, to put it in the larger context of national economic and trade policy to understand the possible consequences.

Business Confidential Information

The line between Business Confidential Information and IP is inexact. Business Confidential Information can include trade secrets or "know how." These categories are similar to IP and their loss imposes similar costs. We distinguish between IP—information that makes it easier to produce a competing product and Business Confidential Information—information that give an advantage in commercial negotiations or in developing competing business strategies.

While it may take years for stolen IP to show up in a competing product, there is no delay in monetizing stolen confidential business information. Theft of oil exploration data, sensitive business negotiation data, or even, insider stock trading information can be used immediately by the acquirer. The damage to individual companies can be great. Measuring this category of loss is very difficult since the victim may not know the reason they were underbid, a negotiation went badly, or a contract was lost.

A more insidious form of hacking is the equivalent of insider trading. In this case, the individual extracting non-public information about a future financial transaction is not an insider, but the effect is the same. Insider trading, or its hacking equivalent, may look like a victimless crime but it reduces social welfare and harm financial markets. An astute hacker may manipulate stock prices or automated trading systems, putting out false news that could affect a price or the market. The effect may be short lived, but a hacker could execute trades planned in advance. In the case of stock manipulation, the cyber crime resembles insider trading which can be notoriously difficult to detect. The information acquired could be used to make trades on another exchange, complicating enforcement efforts.

Cybercrime

While losses due to cybercrime are troubling, they do not directly threaten national security, except to the extent that international cybercrime allows potential opponents to train and maintain proxy forces at others expense. Direct losses to consumers may be the smallest component of the cost of malicious cyber activity. These are usually based on impersonating individuals to gain access to their financial resources or other forms of fraud, such as impersonating an antivirus company in order to persuade individuals to pay to have their computers cleaned.

The UNODC estimates that identity theft is the most profitable form of cyber crime, generating perhaps $1 billion per year in revenue on a global basis.[10] The same UNODC report estimated that the cost of identify theft using cyber techniques in the US was $780 million (data for other countries was not readily available). Data on other kinds of losses by banks is not readily available, but may total in the US, somewhere between $300 million and $500 million a year. This is not an insubstantial loss and if it occurred on our streets there would be an immense outcry. However, financial institutions have regarded this as the cost of doing business in cyberspace.[11]

Service disruptions, such as denial of service attacks, may have only a limited cost on a national economy (although they can be disruptive for the company that experiences them). If the website of an online retailer is taken offline, they will lose sales, but the actual economic effect may be much smaller. Consumers may simply defer a purchase,

10 http://www.unodc.org/toc/en/crimes/organized-crime.html, https://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf. This figure does not include the theft of intellectual property
11 http://www.frbsf.org/banking/audioconf/031413/Call-the-Fed-Cybercrime-3-14-13.pdf

or they may go to another retailer. Even a relatively large denial of service attack, such as those launched against Estonia in 2007, may have only a minimal economic effect. The same is true for extortion schemes where a criminal threatens a denial of service attack or penetrates a network, encrypts data, and then charges a fee for decryption.

A Cambridge University survey of phishing estimated, using figures from Gartner, that the net cost of identity theft for an individual victim is $572, came up with an estimate of $178 million in losses for the 1,400 phishing sites it surveyed. They estimate the total cost to consumers of phishing at $350 million per year. A Gartner report estimated that total annual losses from phishing reached $2 billion per year.[12] The variation in estimates is explained by the differing assumptions used by Cambridge and Gartner. Other estimates conclude that less than one percent of the victims of phishing actually lose money.[13]

A survey of online retailers led to an estimate of $3.5 billion in 2012 for online fraud. As companies have moved to deploy anti-fraud measures, the rate of fraud has fallen by half, from 1.8% in 2004 to 0.9% in 2012. In contrast, losses for mobile commerce are higher, at 1.4%, and these losses are a growing concern for retailers.[14] The overall cost to a national economy is small and would be considered just another form of pilferage if it were not for the risk that these actions could lead to a widespread distrust of the internet and subsequent inability to make further use of it to gain business efficiencies. This has not occurred but it remains a worry for governments.[15] We could quantify this risk by determining the future expected value of internet transactions and the probability that this value would decline if consumers perceived increased risk in internet use.

Cybercrime creates social costs. A website hosting child pornography or advocating terrorism imposes real costs on society. The Congressional Budget Office estimated that the costs of implementing a law to fight child pornography at roughly $30 million a year.[16] This estimate does not of course measure the psychological trauma and "spillover" costs that these activities generate. Intangible costs arise from the suffering of the victims, but this concept needs some adjustment for malicious cyber action. Companies are not persons, although employees or shareholders may suffer as a result of damage from malicious cyber actions (if they are aware that this is the cause). Efforts to estimate the cost of intangible suffering for other crimes suggest another caveat. While average intangible costs may range from millions of dollars for murders to a few dollars for larceny, the intangible costs of forgery fraud or embezzlement are either low or difficult to estimate.[17]

12 An Empirical Analysis of the Current State of Phishing Attack and Defence; http://www.cl.cam.ac.uk/~rnc1/weis07-phishing.pdf p.16

13 http://www.zdnet.com/blog/security/how-many-people-fall-victim-to-phishing-attacks/5084

14 http://www.internetretailer.com/2013/03/28/online-fraud-costs-e-retailers-35-billion-2012

15 The new EU cybersecurity strategy refers to this risk

16 http://www.cbo.gov/sites/default/files/cbofiles/attachments/hr6063.pdf

17 *Intangible costs for stolen property offenses, vandalism, forgery and counterfeiting, embezzlement, and fraud cannot be calculated using available sources.* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2835847/#R12 see Table 4 in particular; https://www.ncjrs.gov/pdffiles1/pr/188070.pdf

Reputational Damage

While companies fear reputation damage, there has been little work to quantify it. Companies suffer reduced valuation after public reporting of their being hacked, usually in the form of a drop in stock prices. These losses can be significant—ranging from 1% to 5%—but appear not to be permanent. Stock prices usually recover by the next quarter. It would distort any calculation of loss to attempt to include these fluctuations in stock prices. However, it will be interesting to see if this changes as a result of new SEC regulations that require companies to report major hacking incidents, which may improve shareholder understanding about what hacks are commercially material. Shareholders are unlikely to have good information about what was taken, let alone by whom and for whose benefit. Recovery of stock prices may not be so quick if investors decide that there has been significant damage to a company's intellectual property portfolio or if it sees a significant outflow of customers as a result.

Increased Cost of Security

It is also necessary to consider, as some studies have done,[18] expenditures on cybersecurity as part of the total cost of cyber espionage and cyber crime. One estimate predicts that governments and companies spend perhaps 7% of their information technology budgets on security. Another estimate put annual spending globally on cybersecurity software at $60 billion, growing at about 8% a year.[19] The US Office of Management and Budget reported that in 2012, federal agencies spent more than $15 billion on cybersecurity-related projects and activities, accounting for 20% of all federal spending on information technology.[20]

As Anderson, et al put it in their very useful study, "We are extremely inefficient at fighting cybercrime; or to put it another way, cyber-crooks are like terrorists or metal thieves in that their activities impose disproportionate costs on society."[21]

Companies will always have to spend on cybersecurity, but if we assume that some percentage of the current spending would be unnecessary in a more secure cyber environment, that additional spending counts as part of the total cost. Determining this "risk premium" for malicious cyber actions faces all the estimation problems in other categories of loss, but one initial reference point would be that companies spent almost a $1 billion in 2012 to insure against the risk of social media attacks, privacy breaches, cyber crime and cyber espionage.[22] This relatively low figure may reflect imperfection in the insurance market as much as company perceptions of cyber risk.[23]

The cost of cleaning up after a cyber attack may be relatively small. One survey found an average of about $9 million for large companies to clean up after a successful breach.[24] Many of those incidents were of the lost-laptop variety, and one might expect the costs of curing actual cyber espionage intrusions to be much higher. One area for further research is increased insurance costs, as companies seek to control liability for breaches of their networks.

Opportunity Costs

A calculation of the cost of malicious cyber activity would need to consider opportunity costs, forgone opportunities, or lost benefits that would otherwise have been obtainable for activities in

---

18 Anderson et al, *Measuring the Cost of Cybercrime, Workshop on the Economics of Cybersecurity,* 2012, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf and http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf

19 Nicole Perlroth, *Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt,* New York Times, December 2012, http://www.nytimes.com/2013/01/01/technology/antivirus-makers-work-on-software-to-catch-malware-more-effectively.html?pagewanted=all; Gartner, Inc., http://www.gartner.com/newsroom/id/2156915, "Gartner Says Security Software Market Grew 7.5 Percent in 2011," April 26, 2012, http://www.gartner.com/it/page.jsp?id=1996415

20 H.R. 1163, Federal Information Security Amendments Act of 2013

21 http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

22 *Global cyber risk premiums near $1 billion,* 15 October 2012, http://insurancenews.com.au/local/global-cyber-risk-premiums-near-1-billion

23 http://www.zyen.com/component/content/article.html?id=966

24 http://www.networkworld.com/news/2012/100812-ponemon-cyberattacks-263113.html

cyberspace. Additional spending on cybersecurity that would not be required in a more secure environment is one example of an opportunity cost. Other examples include lost sales or lower productivity, a decision to avoid the internet for some activities.

A survey cited in the European Commission Cybersecurity Strategy Document found that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases and avoid revealing personal information because of security concerns (the greatest fear is over identity theft for purposes of financial fraud).[25] A 2008 Study commissioned by the European Network and Information Security Agency (ENISA) found "growing public concerns about information security hinder the development of both markets and public services."[26] A 2006 global survey taken by the International Telecommunication Union as part of its campaign to play a greater role in cybersecurity, based on 400 respondents, found that at that time, more than 40% of Internet users avoided some online transactions because of security concerns.[27] None of these figures are determinative, but they suggest that there could be forgone opportunities in the use of the internet for commercial purposes because of security concerns.

We must balance the results of these surveys by noting that internet use continues to grow. When interviewed, individuals express fear or concern but they do not change their behavior. Presumably, internet use could grow at some faster rate if it was more secure. It might be better to say that

weak cybersecurity does not lead people to avoid the internet, but distorts how they use it, leading them to use it for lower value activities than would otherwise be the case. This "distortion" of internet use into lower value activities might be one of the most damaging aspects of cyber espionage and crime.
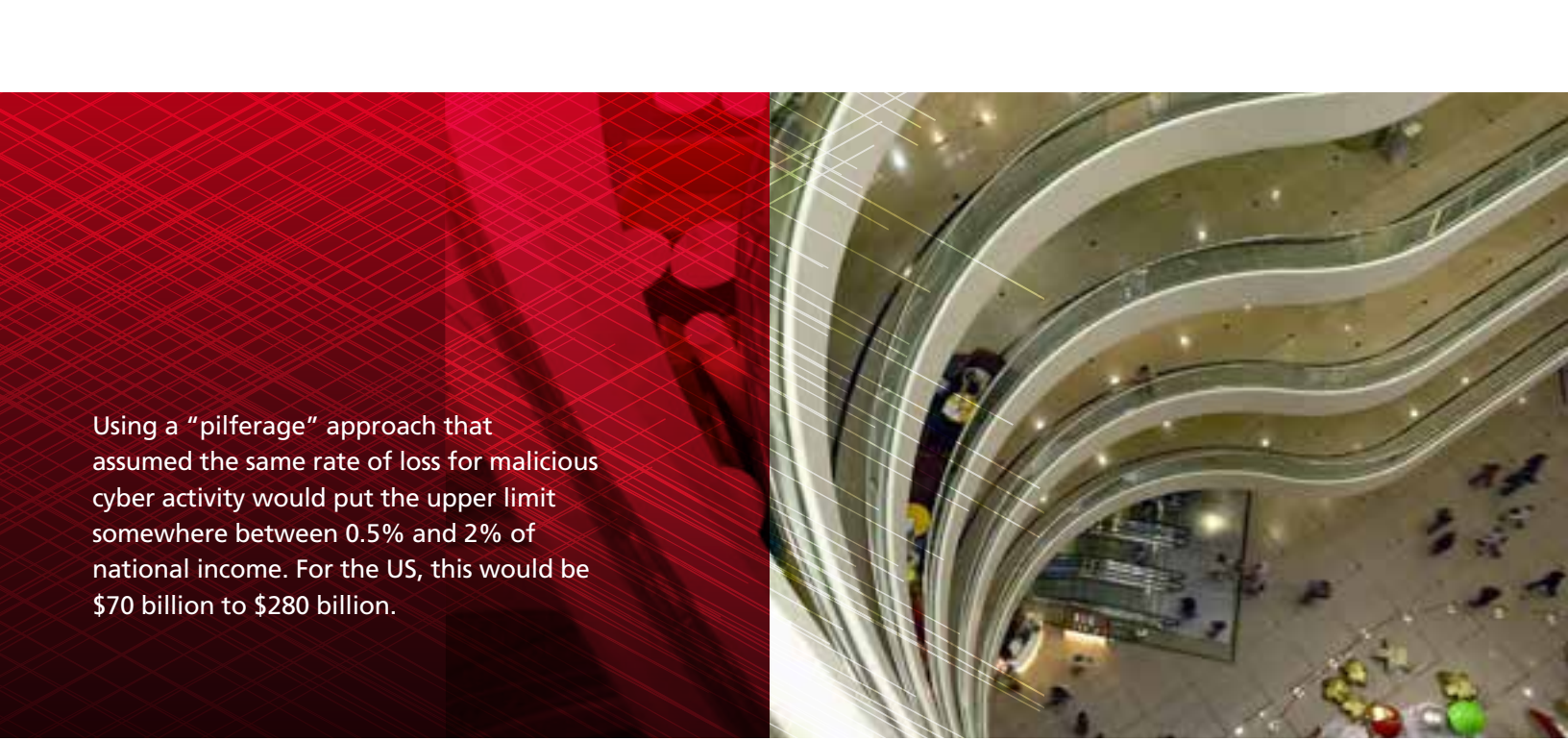
One opportunity cost usually not considered in estimating the damage of cyber crime is the effect on innovation in the receiving country. The theft of intellectual property is a transfer of wealth and knowledge from the victim country to the recipient, improving its ability to produce goods at a lower cost, but it is also likely that this creates disincentives in the recipient country for expanding its own innovative capabilities. This is a corollary to the bromide about teaching a man to fish rather than giving him fish. A man who steals technology will not learn how to create it himself, and eventually the victim of the theft will stop creating new technology as well. One possibility is that cyber espionage harms the recipient country, by disincentivizing innovation, and harms the global capacity to innovate, by both lowering the returns for innovators in the victim country (and thus discouraging them) and by reducing the resources and incentives for innovation in the target country. From this perspective, weak cybersecurity does global harm.

We have not included one potential category of loss—the cost of the "pain and suffering" experienced by the victim. These costs are usually assigned by a court and while some are fixed (such as the cost of a human life in a crash) others can vary widely.

25 2012 Special Eurobarometer 390 on Cybersecurity, http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf
26 http://weis2008.econinfosec.org/papers/MooreSecurity.pdf
27 http://www.itu.int/newsroom/press_releases/2006/09.html

Using a "pilferage" approach that assumed the same rate of loss for malicious cyber activity would put the upper limit somewhere between 0.5% and 2% of national income. For the US, this would be $70 billion to $280 billion.

Using Analogy to Set the Bounds for the Cost of Malicious Cyber Activity

Analogies use a "proxy" number rather than a direct measurement of the phenomena we want to understand. We cannot get data on IP losses, but there is good data on store pilferage, for example, that may let us measure a business decision, the level at which companies decide that losses from an illegal activity are tolerable (noting the difference between high value intangible property and consumer goods). Any proxy is an imperfect facsimile of what we really want to measure, and we need to ask how closely the proxy tracks: knowing how much gas a consumer buys could be a proxy for how many miles they drive, but the results would vary by car model. We would either need a credible "average" gas mileage for all cars or specific data on the types of cars (and their mileage per gallon) that are being driven. Our hope is that by looking at similar problems that are better documented, like crime and disease, we can derive an initial and rough estimate of "ballpark" figures for the costs of malicious cyber activities.

Analogies can provide an idea of the scope of the problem,[28] perhaps allowing us to set rough bounds—a ceiling and a floor—for the cost of malicious cyber activity, by comparing it to other kinds of crime and loss. In looking for analogies that may usefully be compared to malicious cyber activity, we start from the proposition that people will accept substantial costs if they perceive a much greater benefit. Department stores encourage shoppers to touch goods without a salesman present because that boosts sales, even though it also makes shoplifting more likely. Similarly, we all have embraced automobiles despite the risk of crashes. Clearly, societies continue to embrace digitalization despite the risks of cybercrime. The question is whether "tolerated" costs like pilferage or automobile accidents can be used as a guide to the "tolerated" cost of cybercrime.

- **Car Crashes:** The Center for Disease Control estimated (using much better data), the cost of car crashes in the US at $99 billion in 2010. The American Automobile Association estimated the cost of 2010 car crashes at $168 billion. One way to think about the costs of malicious cyber activity is that Americans bear the cost of car crashes as a tradeoff for the convenience of automobiles; similarly they may bear the cost of cyber crime and espionage as a tradeoff for the benefits of information technology. That does not mean it is not in the national interest to try to reduce this loss, and the analogy is imprecise as the theft of sensitive military technology creates damage

28 http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

whose full cost is not easily quantifiable in monetary terms. As with car crashes, we may also wish to consider if the monetary costs accurately reflect the cost of "pain and suffering" experienced by the victim if they realize they have been hacked.

- **Piracy:** A weakly governed space exploited by criminals could describe some oceanic areas as well as the internet. The Somali coast is the best known example but there are other locations. The International Maritime Bureau, a nongovernmental organization that is part of the International Chamber of Commerce, tracks incidents of piracy around the world. It estimated the annual cost of piracy as somewhere between $1 billion and $16 billion in 2005 (apparently cyber is not the only field where estimation is difficult). Another group estimated that piracy cost the global economy between $7 to $12 billion in 2010.[29] There are also human costs that are not reflected in these estimates that include captivity for long periods and in a few instances, death among the crews of ships seized by pirates, increased insurance costs, and opportunity costs as captured ships are unable to earn income and often damaged. To put these figures in context, the annual value of maritime trade in 2005 was $7.8 trillion, which means piracy costs equaled at most 0.02 percent of the total and probably less.[30]

- **Pilferage:** Another approach to estimating loss might begin by noting that many industries have reacted lethargically to cyber espionage. Perhaps these companies have made a rational calculation, similar to that made by retail stores, that the cost of preventing all losses is simply greater than the losses themselves. Companies accept rates of "pilferage" or "inventory shrinkage" as an operating cost. For retail companies in the US, this falls between 1.5% and 2.0% of annual sales—a 2008 estimate put pilferage losses at 1.7%. Using a "pilferage" approach that assumed the same rate of loss for malicious cyber activity would put the upper limit somewhere between 0.5% and 2% of national income. For the US, this would be $70 billion to $280 billion. It is possible that companies may have made a rational calculation of where it makes business sense to improve their cyber

defenses, similar to that made by retail stores on pilferage.[31] A central problem for the "pilferage theory," however, is that many companies do not know the extent of their losses, leading to a rational business decision based on inadequate information.

- **Crime and Drugs:** One frequently heard comparison is that malicious cyber activity is more lucrative than the drug trade. This begs the question of whether we actually know the value of the drug trade. In October 2012 the UN Office on Drugs and Crime estimated the cost of all transnational organized crime as $870 billion, or 1.2% of global GDP.[32] It estimated $600 billion of this figure came from illegal drug trafficking. The remaining $270 billion accounts for all other kinds of transnational crime, including human trafficking, smuggling, and cyber crime. In places where the drug trade flourishes, we can see marked social and economic effects. Cyber crime does not produce similar observable effects. Saying that malicious cyber activity generates more than $600 billion seems to be an exaggeration.

The Limits of Analogy

If we are right in assuming that "tolerated costs" from malicious cyber activity falls into the same range as car crashes, pilferage, and drugs, this provides ballpark figures setting a "ceiling" for any estimate of loss from cybercrime. They seem to suggest that the most that cybercrime and cyber espionage could cost is 1% or less of GDP. This rests on untested assumptions about how cyber activities correlate with other tolerated losses, and on the extrapolation of broad trends from a few uncertain data points, the utility of illicitly acquired IP, and the accuracy of reported losses from cyber crime and espionage. It likely overestimates the losses to developing nations, which are neither as IP-intensive nor as reliant on networks. Any loss is likely not distributed evenly across firms and countries, suggesting that some individual nations and companies bear a heavier burden. As with any modeling effort, vary the assumptions and the model's output will be different. Greater precision in these assumptions could lead to significantly different results, but any estimate that goes beyond this ceiling deserves careful scrutiny. We welcome comments and criticism of this approach.

29 http://oceansbeyondpiracy.org/sites/default/files/documents_old/The_Economic_Cost_of_Piracy_Full_Report.pdf
30 http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG697.pdf
31 http://dcipattorney.com/2010/12/the-us173-4b-global-intellectual-property-marketplace/
32 http://www.unodc.org/unodc/en/frontpage/2012/October/transnational-crime-proceeds-in-billions-victims-in-millions-says-unodc-chief.html

What's the Harm?

This initial research suggest an upper limit of the cost of cyber espionage and crime somewhere between 0.5% and 1% of national income—for the US, this would be about $70 billion to $140 billion. A lower limit might be $20 billion to $25 billion. This is a very broad range and we hope that our future work can narrow it. A starting point for a better estimate would be to reduce the reliance on anecdotes and surveys, and begin to compile and compare existing estimates, develop better data on value, and refine assumptions about loss. While a precise single figure for the cost of cyber crime and cyber espionage is unattainable, a more accurate estimate of the range of potential losses can be developed, allowing us to better measure the problem.

A very crude extrapolation would be to take this range for the US, which accounts for a little more than a fifth of global economic activity, and come up with a range of $100 billion to $500 billion for global losses. This is almost certainly an overestimate. An initial adjustment would be to note that less developed economies rely less on networks and have less intangible property than developed economies. In just the ten leading economies the value of "intangible" goods and services ranges from 50% to 70% of GDP; taking this into account would suggest a range of $80 billion to $400 billion in global losses. This range is so broad we offer them only as a starting point for further research on the global effect of malicious cyber activity. In the context of a $70 trillion global economy, these losses are small, but that does not mean it is not in the national interest to try to reduce the loss, and the theft of sensitive military technology creates damage whose full cost is not easily quantifiable in monetary terms.

We also need to disentangle the ordinary transfer of technology that is a normal part of foreign investment. Cyber espionage is best seen as a troubling addition to this larger trend of global technology transfer. We do not want to ascribe all technology transfer and increases in foreign competitiveness to cyber espionage, nor do we want to ignore the possibility that cyber espionage can, over the long term, dramatically affect on economic growth, where even a few tenths of a percentage point over a number of years can change a nation's economic health.

Companies have likely underestimated the risk they face. Some companies believe that the damage from espionage is tolerable, part of the cost of doing business in the world's fastest growing markets, and that they can "run faster," to create new technologies and so minimize any loss. There may have been an economic rationale for this, in that for an individual firm, there are near term gains. But illicit technology transfer, even if the technology is dated by US standards, accelerates military modernization. It accelerates improvements in indigenous industrial and technological capabilities, making the recipient better able to absorb stolen technology in the future and produce competitive products. Companies risk losing not just their strategic advantage, not just intellectual property but also customer lists, their competitive analyses, and sales data.

The dollar value of malicious cyber activity may understate the actual damage if there is a "multiplier effect." There are proponents of government-funded research who argue strenuously, albeit self-interestedly, that a dollar spent on research produces more than a dollar of economic benefit. If this is true, the multiplier effect for cyber espionage could be far greater if the research is acquired for free. The loss of a dollar of IP due to cyber espionage

could produce more than a dollar of benefit for a foreign competitor. If this is accurate, the lost of $20 billion in intellectual property translates into a much greater benefit for the acquiring nation. But this is uncertain ground, as the estimation of a multiplier effect remains in dispute in economic literature. Some economists assert that one dollar spent on biomedical research, for example, produces two dollars in benefits. Other estimates by critics of the multiplier effect suggest that one dollar in spending may have a multiplier effect of only 80 cents or even less.[33]

As noted earlier, another difficulty lies in quantifying the dollar cost of damage to national security. First, there is a link between cyber espionage and the development of cyber attack capabilities. Cyber espionage provides, if nothing else, knowledge of potential targets and training for attackers. Second, there is a link between cyber espionage directed at commercial targets and cyber espionage targeted on military technology. It is often the same actors pursuing a collection plan that targets both military and commercial sources. In the US, for example, a strong case could be made that there has been extensive damage to the US lead in stealth, submarine, missile, and nuclear capabilities. We cannot accurately assess the dollar value of the loss in military technology but we can say that cyber espionage, including commercial espionage, shifts the terms of engagement in favor of foreign competitors.

Terms of Trade and the Effect on Employment

Terms of trade refers to how much a country must export in order to pay for its imports. If imports fall in value, the terms of trade shift in favor of the importing country, as it will have to export fewer goods than before to pay its bills. Before we leap to the conclusion that stolen intellectual property will eventually mean lower prices for consumers, we should consider several caveats. First, many people will find it absurd to take account of the "benefits" of criminal acts. Second, cyber espionage reduces the comparative advantage of research, education, and know-how, making it harder for victim nations with advanced economies to produce the goods they need to pay their import bills. Even though the effect of cyber espionage is to "subsidize" foreign production, the benefits to consumers in the victim country are likely to be small.

If the workers displaced by cyber espionage do not find jobs that pay as well or better, the victim country would be worse off. Analysis by the Commerce Department's International Trade Administration found that in 2011, $1 billion in exports equaled 5,080 jobs.[34] Since the total number of workers in the United States ranges between 135 million to 145 million, this means that the high-end estimate of $100 billion in losses from cyber espionage would translate into 508,000 lost jobs and the effect of cyber espionage on employment might be roughly a third of a percent decrease in employment.

Rather than the aggregate number of jobs, the real concern might be if the lost jobs are in manufacturing or other high paying sectors. The effect of cyber espionage may be to move US workers from high paying blue collar jobs into lower paying work or even unemployment. More importantly, if our rough estimates of loss and of the cost in jobs are right, and since they are relatively small, it may point to the real damage from the theft of intellectual property. The greatest damage and risk from malicious cyber activity may not be in terms of direct damage to the victim country, but the illicit benefit obtained by the acquiring country, whose economic development and ability to compete globally (economically and perhaps militarily) are increased and accelerated through illegitimate means.

33 http://www2.isu.edu/headlines/?p=1283; http://www.bea.gov/regional/rims/brfdesc.cfm; Barro, http://online.wsj.com/article/SB123258618204604599.html

34 International Trade Administration, *Jobs Supported by Exports: An Update,* March 12, 2012, http://www.trade.gov/mas/ian/build/groups/public/@tg_ian/documents/webcontent/tg_ian_003639.pdf

Next Steps for Estimation

We have identified important factors for determining the cost of malicious cyber activity.

These factors may be quantifiable, but they rest on assumptions about the utility of illicitly acquired IP and the accuracy of reported losses from cyber crime and espionage. A precise single figure for the cost of cyber crime and cyber espionage is unattainable, but a more accurate estimate of the range of potential losses can be developed.

We have also identified a number of issues that affect measurement and effect. Putting a number on the cost of cybercrime and cyber espionage is the headline, but the heart of the matter is the effect on trade, technology, and competitiveness. Our next report will provide a range of estimates, using a variety of techniques, models, and assumptions, but it will also assess these larger and more consequential effects. We plan in the final report to use data from other nations and refine our estimates of loss. In particular, we will analyze four fundamental questions:

- Can "tolerated cost" analogies of sufficient accuracy be developed to let us estimate the costs of cybercrime? One proxy of possible interest starts from the proposition that the implicit cost-benefit analysis of "tolerated costs" may be skewed by immediate gratification in the context of computer adoption. Individuals may willingly incur much heavier, and arguably irrational, losses if they are making choices between short-term gratification and long-term costs. Health care and other costs associated with preventable disease may fit this model. What costs are incurred as a result of life-style choices—smoking, obesity, lack of exercise—that many of us know are not healthy but which are irresistible in the moment. (Smoking of course is addictive, but so, some would say, is … excuse me but I have to check my Twitter feed.)

- Is the illicit acquisition of technology through cyber means a significant technology gain for the attackers that poses long-term costs to the victim economy, or does hacking produce only marginal changes in economic activity by both victim and attacker (noting that the effect on individual companies may be ruinous)?
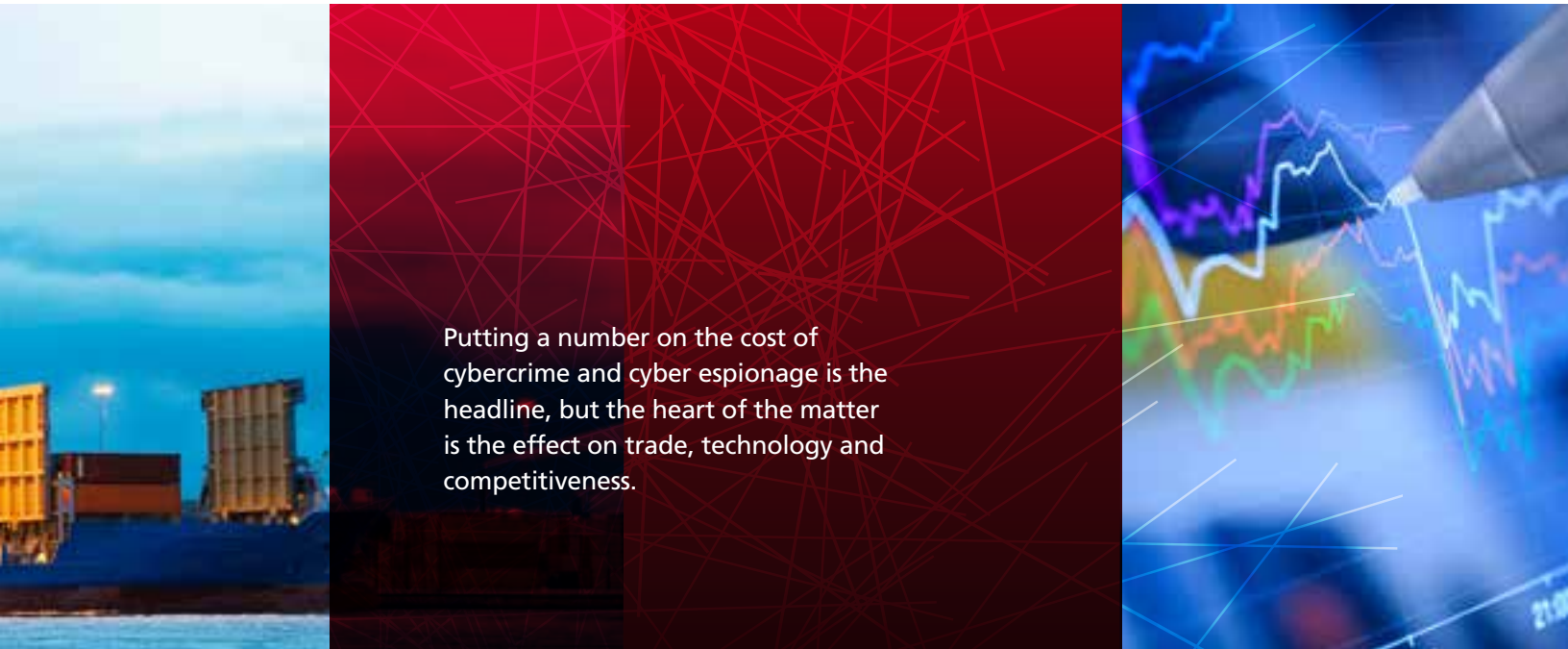
> Putting a number on the cost of cybercrime and cyber espionage is the headline, but the heart of the matter is the effect on trade, technology and competitiveness.

- Do companies discount the cost as a normal part of business, or are they unaware of the real scale of loss and damage?
- Is dollar cost for losses an accurate measure of the effect of cyber espionage and cyber crime, or does this undervalue intangible costs, including trust in the international system or the effect on military power?

Answering these larger questions, will help us scope the problem and put it in a strategic context. Cybercrime and cyber espionage cost the global economy billions of dollars every year. The dollar amount, large as it is likely to be, may not fully reflect the damage to the global economy. Cyber espionage and crime slows the pace of innovation, distorts trade, and brings with it the social costs associated with crime and job loss. This larger effect may be more important than any actual number and it is one we will focus on in our final report.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe.

http://www.mcafee.com

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, non-profit organization founded in 1962 and headquartered in Washington, D.C. It seeks to advance global security and prosperity by providing strategic insights and policy solutions to decision makers.

This report is authored by James Lewis, Director and Senior Fellow, Technology and Public Policy Program, CSIS and Stewart Baker, CSIS and Partner, Steptoe & Johnson LLP.