Critical Infrastructure Protection in Homeland Security

Defending a Networked Nation

Third Edition

Ted G. Lewis

with website

WILEY

CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY

CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY

Defending a Networked Nation

Third Edition

TED G. LEWIS

WILEY

Edition History
John Wiley & Sons Inc. (1e, 2006)
John Wiley & Sons Inc. (2e, 2015)

Registered Office
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA

Editorial Office
111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Limit of Liability/Disclaimer of Warranty
In view of ongoing research, equipment modifications, changes in governmental regulations, and the constant flow of information relating to the use of experimental reagents, equipment, and devices, the reader is urged to review and evaluate the information provided in the package insert or instructions for each chemical, piece of equipment, reagent, or device for, among other things, any changes in the instructions or indication of usage and for added warnings and precautions. While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials or promotional statements for this work. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Library of Congress Cataloging-in-Publication Data

Names: Lewis, T. G. (Theodore Gyle), 1941– author.
Title: Critical infrastructure protection in homeland security : defending
a networked nation / Theodore Gyle Lewis.
Description: Third edition. | Hoboken, NJ : John Wiley & Sons Inc., 2020. |
Includes bibliographical references and index.
Identifiers: LCCN 2019032791 (print) | LCCN 2019032792 (ebook) | ISBN
9781119614531 (hardback) | ISBN 9781119614555 (adobe pdf) | ISBN
9781119614562 (epub)
Subjects: LCSH: Computer networks–Security measures–United States. |
Computer security–United States–Planning. | Terrorism–United
States–Prevention. | Terrorism–Government policy–United States. |
Civil defense–United States. | Public utilities–Protection–United
States.
Classification: LCC QA76.9.A25 L5 2020 (print) | LCC QA76.9.A25 (ebook) |
DDC 005.8–dc23
LC record available at https://lccn.loc.gov/2019032791
LC ebook record available at https://lccn.loc.gov/2019032792

Cover design by Wiley
Cover image: © SERGII IAREMENKO/SCIENCE PHOTO LIBRARY/Getty Images

Set in 10/12pt Times by SPi Global, Pondicherry, India

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

CONTENTS

FOREWORD BY SEN. MARK WARNER

“Today, December 7th, is an auspicious date in our history. We remember Pearl Harbor as the first foreign attack on US soil in modern history. Unfortunately, we also remember Pearl Harbor as a major intelligence failure. As Vice Chairman of the Intel Committee, I’ve spent the better part of the last two years on an investigation connected to America’s most recent intelligence failure. It was also a failure of imagination—a failure to identify Russia’s broader strategy to interfere in our elections. Our federal government and institutions were caught flat-footed in 2016, and our social media companies failed to anticipate how their platforms could be manipulated and misused by Russian operatives. Frankly, we should have seen it coming.

Over the last two decades, adversary nations like Russia have developed a radically different conception of information security—one that spans cyber warfare and information operations. I fear that we have entered a new era of nation-state conflict: one in which a nation projects strength less through traditional military hardware and more through cyber and information warfare. For the better part of two decades, this was a domain where we thought we had superiority. The thinking was that our cyber capabilities were unmatched. Our supposed superiority allowed us to write the rules.

This confidence appears to have blinded us to three important developments: First, we are under attack, and candidly, we have been for many years. Our adversaries and their proxies are carrying out cyber attacks at every level of our society. We’ve seen state-sponsored or sanctioned attacks on healthcare systems, energy infrastructure, and our financial system. We are witnessing constant intrusions into federal networks. We’re seeing regular attempts to access parts of our critical infrastructure and hold them ransom. Last year, we saw global ransomware attacks increase by 93%. Denial-of-service attacks increased by 91%. According to some estimates, cyber attacks and cybercrime account for up to $175 billion in economic and intellectual property loss per year in North America. Globally, that number is nearly $600 billion. Typically, our adversaries aren’t using highly sophisticated tools. They are attacking opportunistically using phishing techniques and rattling unlocked doors. This has all been happening under our noses. The effects have been devastating, yet the attackers have faced few, if any, consequences.

Second, in many ways, we brought this on ourselves. We live in a society that is becoming more and more dependent on products and networks that are under constant attack. Yet the level of security we accept in commercial technology products is unacceptably low—particularly when it comes to rapidly growing Internet of Things. This problem is only compounded by our society-wide failure to promote cyber hygiene. It is an outrage that more digital services from email to online banking don’t come with default two-factor authentication. And it is totally unacceptable that large enterprises—including federal agencies—aren’t using the available tools.

Lastly, we have failed to recognize that our adversaries are working with a totally different playbook. Countries like Russia are increasingly merging traditional cyber attacks with information operations. This emerging brand of hybrid cyber warfare exploits our greatest strengths—our openness and free flow of ideas. Unfortunately, we are just now waking up to it. Looking back, the signs should have been obvious. Twenty years ago, Sergei Lavrov, then serving as Russia’s UN Ambassador, advanced a draft resolution dealing with cyber and prohibiting particularly dangerous forms of information weapons. We can debate the sincerity of Russia’s draft resolution, but in hindsight, the premise of this resolution is striking. Specifically, the Russians saw traditional cyber warfare and cyber espionage as interlinked with information operations. It's true that, as recently as 2016, Russia continued to use these two vectors—cyber and information operations—on separate tracks. But there is no doubt that Putin now sees the full potential of hybrid cyber operations. By contrast, the United States spent two decades treating information operations and traditional information security as distinct domains. Increasingly, we treated info operations as quaint and outmoded. Just a year after Lavrov introduced that resolution, the United States eliminated the United States Information Agency, relegating counterpropaganda and information operations to a lower tier of foreign policy. In the two decades that followed, the United States embraced the Internet revolution as inherently democratizing. We ignored the warning signs outside the bubble of Western democracies.

The naïveté of US policy makers extended not just to Russia, but to China as well. Recall when President Clinton warned China that attempts to police the Internet would be like nailing Jell-O to the wall. In fact, China has been wildly successful at harnessing the economic benefits of the Internet in the absence of political freedom. China's doctrine of cyber sovereignty is the idea that a state has the absolute right to control information within its border. This takes the form of censorship, disinformation, and social control. It also takes the form of traditional computer network exploitation. And China has developed a powerful cyber and information affairs bureaucracy with broad authority to enforce this doctrine. We see indications of the Chinese approach in their successful efforts to recruit Western companies to their information control efforts. Just look at Google's recent push to develop a censored version of its search engine for China. Today, China's cyber and censorship infrastructure is the envy of authoritarian regimes around the world. China is now exporting both its technology and its cyber-sovereignty doctrine to countries like Venezuela, Ethiopia, and Pakistan. With the export of these tools and ideas, and with countries like North Korea and Iran copying Russia's disinformation playbook, these challenges will only get worse. And yet as a country we remain complacent.

Despite a flurry of strategy documents from the White House and DoD, the federal government is still not sufficiently organized or resourced to tackle this hybrid threat. We have no White House cyber czar, nor cyber bureau or senior cyber coordinator at the State Department. And we still have insufficient capacity at State and DHS when it comes to cybersecurity and disinformation. Our Global Engagement Center at the State Department is not sufficiently equipped to counter propaganda from our adversaries. And the White House has still not clarified roles and responsibilities for cyber across the US government. While some in the private sector have begun to grapple with the challenge, many more remain resistant to the changes and regulations needed. And the American people—still not fully aware of the threat—have not internalized the lessons of the last few years. We have a long way to go on cyber hygiene and online media consumption habits. Let me be clear: Congress does not have its act together either. We have no cyber committee. Cyber crosses numerous committee jurisdictions frequently hindering our ability to get ahead of the problem.

It's even worse in the area of misinformation/disinformation. The dangers are only growing as new technologies such as Deepfakes audio and video manipulation that can literally put words into someone's mouth are commercialized. The truth is, we are becoming ever more dependent on software. But at the same time, we are treating cybersecurity, network resiliency, and data reliability as afterthoughts. And these vulnerabilities will only continue to grow as our so-called real economy becomes increasingly inseparable from the digital economy.

If we're going to turn this around, we need not just a whole-of-government approach; we need a whole-of-society cyber doctrine. So what would a US cyber doctrine look like? It's not enough to simply improve the security of our infrastructure, computer systems, and data. We must also deal with adversaries who are using American technologies to exploit our freedom and openness and attack our democracy.

Let me lay out five recommendations:

1 NEW RULES

First, we need to develop new rules and norms for the use of cyber and information operations. We also need to better enforce existing norms. And most importantly, we need to do this on an international scale. We need to develop shared strategies with our allies that will strengthen these norms. When possible, we need to get our adversaries to buy into these norms as well. The truth is, our adversaries continue to believe that there won't be any consequences for their actions. In the post-9/11 national security environment, we spent tremendous energy combating terrorism and rogue states. But frankly, we've allowed some of our near-peer adversaries to operate with relative impunity when they attack the United States in the digital domain. There have been some reports in the press about the United States supposedly punching back at second-tier adversaries on occasion. But we've largely avoided this with Russia and China out of a fear of escalation. If a cyber attack shuts down Moscow for 24 h with no power, that's a problem. If someone were to shut down New York for 24 h, that would be a global crisis. As a result, for Russia and China, it's pretty much been open season on the United States. That has to end.

We need to have a national conversation about the defensive and offensive tools we are willing to use to respond to the ongoing threats we face. In short, we need to start holding our adversaries accountable. Failing to articulate a clear set of expectations about when and where we will respond to cyber attacks is not just bad policy, but it is downright dangerous. We are allowing other nations to write the playbook on cyber norms. Part of this is the result of US inaction: from the late 1990s into the early 2000s, the United States was a consistent dissenting voice in UN meetings where cyber norms were proposed. In part, this reflected our aversion to piecemeal approaches to cybersecurity. But it also reflected a view that we didn't want to be bound by lesser powers. In 2015, there was a major effort at the UN—including the United States—to agree to principles of state behavior in cyberspace. We saw some international consensus around protecting critical infrastructure and investigating and mitigating cybercrime. Unfortunately, those 2015 principles at the UN failed to address economic espionage. And even the 2015 US–China cyber espionage deal was insufficient. And in 2017, disagreements between the United States, China, and Russia at the UN led to a deadlock on the question of how international law should apply to cyber conflicts. Little progress has been made since then.

It's true that some folks in the private sector and the NGO space have stepped up. Look at Microsoft's Digital Geneva Convention. Look at the recent Paris Call for Trust and Security in Cyberspace—signed by 57 nations, but not by the United States. This is yet another example of the United States stepping back on the world stage, with countries like France filling the void.

Recently, the US government and the State Department, in particular, have renewed efforts to advance a norms discussion. These efforts must be elevated and strengthened. But norms on traditional cyber attacks alone are not enough. We also need to bring information operations into the debate.

This includes building support for rules that address the Internet's potential for censorship and repression. We need to present alternatives that explicitly embrace a free and open Internet. And we need that responsibility to extend not only to government, but to the private sector as well. We need multilateral agreements with key allies, just like we've done with international treaties on biological and chemical weapons. That discussion needs to address mutual defense commitments.

We should be linking consensus principles of state behavior in cyberspace, explicitly, with deterrence and enforcement policies. US policy makers, with allies, should predetermine responses for potential targets, perpetrators, and severity of attack. That means clearly and publicly linking actions and countermeasures to specific provocations. That could mean sanctions, export controls, or indictments. It could even include military action or other responses. Now, we should be realistic about the limits of norms in shaping behavior.

Let's not kid ourselves: in the short term, a nation like Russia that routinely ignores global norms is not going to make an about-face in the cyber domain. This should not deter us, but it should give us a more realistic set of expectations for how quickly we can expect to see results. But the stronger we make these alliances, the more teeth we can apply to these norms, and the more countries we can recruit to them, the more effective these efforts will be at disciplining the behavior of Russia, China, and other adversaries.

2 COMBATING MISINFORMATION AND DISINFORMATION

My second recommendation is: we need a society-wide effort to combat misinformation and disinformation, particularly on social media. My eyes were really opened to this through the Intel Committee's Russia investigation. Everyone on the Committee agrees that this linkage between cyber threats and disinformation is a serious challenge—especially on social media. In some ways, this was a whole new world for the IC. It is now clear that foreign agents used American-made social media to spread misinformation and hijack our civil discourse.

Let's recap. The Russian playbook included:

- Cyber penetrations of our election infrastructure;
- Hacks and weaponized leaks;
- Amplification of divisive, pro-Kremlin messages via social media;
- Overt propaganda;
- Funding and supporting extreme candidates or parties; and
- Misinformation, disinformation, and actual fake news.

The goal was, and is, to undermine our faith in the facts—our faith in the news media—and our faith in the democratic process. This is an ongoing threat, and not just to the United States. We've also seen these tools used against other Western democracies. We've seen them used to incite racial and ethnic violence in places like Myanmar. This threat is particularly serious in countries with low media literacy. In many ways, social media IS the Internet in some of these countries. So, what do we do? How do we combat this threat? We can start by recognizing that this is a truly global problem. A twenty-first-century cyber and misinformation doctrine should lean into our alliances with NATO countries and other allies who share our values.

Earlier this year, Senator Rubio and I brought together a group of 12 parliamentarians from our NATO allies at the Atlantic Council. We held a summit focused on combating Russian election interference. Ironically, this was the very same day that our President stood on stage and kowtowed to

Vladimir Putin in Helsinki. Meanwhile, we were working with our NATO allies to develop a road map for increased cooperation and information sharing to counter Russian cyber and misinformation/disinformation aggression. In many cases, these countries are further along in educating their populations about the threat of misinformation and disinformation.

Last month, I met with the Prime Minister of Finland. As he put it, the Finns have been dealing with Russian misinformation and disinformation for over a 100 years. Finland is one of the most resilient countries when it comes to countering this threat from its neighbor to the east. Why is that? Again, it is their whole-of-society approach. It relies on a free press that maintains trust through strong self-regulatory mechanisms and journalistic standards. It places limits on social media platforms. They also have a vibrant digital civics initiative.

Finland's approach also depends on national leadership that stays true to its values—even in the midst of contested elections and its own brand of partisan politics. Here in the United States, it will take all of us—the private sector, the government, including Congress, and the American people—to deal with this new and evolving threat.

In terms of the private sector, the major platform companies—like Twitter and Facebook, but also Reddit, YouTube, and Tumblr—aren't doing nearly enough to prevent their platforms from becoming petri dishes for Russian disinformation and propaganda.

I don't have any interest in regulating these companies into oblivion. But as these companies have grown from dorm-room startups into media behemoths, they have not acknowledged that their power comes with great responsibility. Recall that immediately following the election, Mr. Zuckerberg publicly ridiculed the idea that Russia had influenced the US election via Facebook as a "pretty crazy idea."

Now, I don't have all the solutions. But I expect these platforms to work with us in Congress so that together we can take steps to protect the integrity of our elections and our civil discourse in the future. Companies like Facebook and Twitter have taken some helpful voluntary steps—but we need to see much more from them.

That's going to require investments in people and technology to help identify misinformation before it spreads widely. I've put forward a white paper, which lays out a number of policy proposals for addressing this: we can start with greater transparency. For example, I think folks have the right to know if information they're receiving is coming from a human or a bot. I've also put forward legislation called the Honest Ads Act that would require greater transparency and disclosure for online political ads.

Companies should also have a duty to identify inauthentic accounts—if someone says they're Mark from Alexandria but it's actually Boris in St. Petersburg, I think people have a right to know. We also need to put in place some consequences for social media platforms that continue to propagate truly defamatory content. I think platforms should give greater access to academics and other independent analysts studying social trends like disinformation. We also discuss in that paper a number of other ideas in the white paper around privacy, price transparency, and data portability. These are ideas intended to spark a discussion, and we need social media companies' input. But we're moving quickly to the point where Congress will have no choice but to act on its own. One thing is clear: the wild west days of social media are coming to an end.

3 HARDEN NETWORKS, WEAPONS SYSTEMS, AND IOT (INTERNET OF THINGS)

Third, we need to harden the security of our computer networks, weapons systems, and IoT devices. Many of the responsibilities for cyber and misinformation/disinformation will fall on the government. But our nation's strategic response must also include greater vigilance by the private sector, which has frequently resisted efforts to improve the security of its products.

For over a decade, the United States thought it could set a light-touch standard for global data protection by avoiding any legislation. While regulation can have costs, what we've learned is that US inaction can also have costs—as other jurisdictions leap ahead with more stringent privacy and data protections.

We see this with GDPR, where the US failure to adopt reasonable data protection and privacy rules left the field open for much stricter European rules. These standards are now being adopted by major economies like Brazil, India, and Kenya. More broadly, we need to think about a software liability regime that drives the market toward more secure development across the entire product lifecycle. But nowhere is the need for private sector responsibility greater than the Internet of Things. General Ashley, Director of the DIA, has described insecure IoT and mobile devices as the most important emerging cyber threat to our national security.

As a first step, we should use the purchasing power of the federal government to require that devices meet minimum security standards. I have legislation with Senator Cory Gardner to do this. At least at the federal level, we need to make sure that these devices are patchable. We need to make sure they don't have hard-coded passwords that cannot be changed. We need standards to make sure they're free of known security vulnerabilities. And on a broader level, public companies should have at least one board member who can understand and model cyber risk.

Another area I've been working on is trying to impose some financial penalties on companies like Equifax who fail to take the necessary steps to secure their systems from cyber intrusions. Unfortunately, even in areas where we would expect a higher level of security and cyber hygiene, we find these same problems. In October, a GAO report found that "nearly all" of our new weapons systems under development are vulnerable to attack.

Earlier this year, we successfully included language in the NDAA requiring cyber vulnerability assessments for weapons systems, which hopefully should help correct this. The Pentagon has also taken steps recently to make cybersecurity a greater priority within DoD, but frankly we face some serious workforce challenges in recruiting and retaining the top cyber professionals who have plenty of lucrative opportunities in the private sector.

4 REALIGN DEFENSE SPENDING

This is a good segue to my fourth recommendation: realigning our defense spending priorities. The US military budget is more than $700 billion, while Russia spends roughly $70 billion a year on their military. The United States is spending it mostly on conventional weapons and personnel. By contrast, Russia devotes a much greater proportion of its budget to cyber and other tools of asymmetric warfare like disinformation. Russia has come to the realization that they can't afford to keep up with us in terms of traditional defense spending. But when it comes to cyber, misinformation, and disinformation, candidly Russia is already a peer adversary.

A matter of fact, if you add up everything Russia spent on election interference in 2016 and double it, that's still less than the cost of one new F-35. I worry we may be buying the world's best twentieth-century military hardware without giving enough thought to the twenty-first-century threats we face. And it's a similar story with China. China spends roughly $200 billion on defense, but it spends a greater proportion on cyber misinformation and disinformation. If you look at the delta between what we're spending and what China is spending on defense, they're investing more in AI, quantum computing, 5G, and other twenty-first-century technologies. Frankly, they are outpacing us by orders of magnitude. We need to realign our priorities while we still can. Some of DoD's budget should be redirected toward cyber defense. But we also need efforts at other agencies, including R&D funding for quantum computing and AI, as well as investments in cyber technology and cyber workforce development.

5 PRESIDENTIAL/GOVERNMENT LEADERSHIP

The final point is that we desperately need strong federal and presidential leadership for any US cyber doctrine to be truly effective. Because this challenge literally touches every aspect of our society, we need presidential leadership and a senior coordinating official to head the interagency process on this issue.

It's true there are men and women within DoD, DHS, and other agencies who are working hard to defend the United States from cyber attacks. But only the President can mobilize the whole-of-society strategy we need. I do want to acknowledge some positive steps that have been taken in recent months.

The White House and DoD have released two important strategic documents on cyber strategy that move us in the right direction. I also welcome the delegation of authorities to defend and deter cyber attacks below the presidential level. This has allowed for quicker responses and greater interagency coordination. But frankly, these efforts are inadequate.

In the most recent NDAA, Congress attempted to establish a more aggressive posture on US cybersecurity policy. This includes the potential use of offensive cyber capabilities to deter and respond to cyber attacks against US interests—as well as authorization to combat info operations. It also grants the President and Defense Secretary authority to direct Cyber Command to respond and deter "an active, systematic, and ongoing campaign of attacks" carried out by Russia, China, North Korea, and Iran. These powers, if used correctly, are important components of a cyber doctrine. But by definition they require thoughtful, decisive leadership at the top.

I'll leave you with some final thoughts. More broadly, we need a coherent strategy for how to deal with the hybrid approach of our adversaries. Let me be clear about what I'm not saying: I am not advocating that the United States mimic the approach of Russia and China—the idea that states have a sovereign right to control or censor information within their borders. Frankly, that vision is incompatible with our American values and our Constitution.

What I am saying is that we need to confront the fact that our adversaries have an approach that considers control of information an essential component of their overall strategies. We have not only failed to recognize this situation, but over the last two decades we have tended to minimize the dangers of information operations. The truth is, the 2016 presidential election served as a wake-up call in the use of cyber attacks and information operations.

People keep warning of a "digital Pearl Harbor" or a "digital 9/11" as if there will be a single extraordinary event that will force us to action on these issues. But I have news for you: we are already living these events. They're happening every day. Look at the 2017 NotPetya attack. In the United States, we treated this as a one-day news story, but the global cost of that one attack is over $10 billion. This is the most costly and devastating cybersecurity incident in history, and most Americans have no idea. But the true costs of our cyber vulnerabilities won't be sudden or catastrophic. They will be gradual and accumulating. Our personal, corporate, and government data is being bled from our networks every day; our faith in institutions and our tolerance for one another is being eroded by misinformation. This is leaving us exposed as individuals and vulnerable as a country. It's time we dramatically shift how we view these threats. I hope the ideas I've laid out today will help us move toward the comprehensive cyber doctrine that we so desperately need in these challenging times."

FOREWORD BY PROF. ANDREW ODLYZKO

Cybersecurity Is Not Very Important

Andrew Odlyzko
University of Minnesota
odlyzko@umn.edu http://www.dtc.umn.edu/∼odlyzko Revised version, March 9, 2019.

> A New Doctrine for Cyberwarfare and Information Operations, Center for New American Security, Sen. Mark R. Warner, December 7, 2018

1 INTRODUCTION

It is time to acknowledge the wisdom of the "bean counters." For ages, multitudes of observers, including this author, have been complaining about those disdained accountants and business managers. They have been blamed for placing excessive emphasis on short-term budget constraints, treating cybersecurity as unimportant, and downplaying the risks of disaster.

With the benefit of what is now several decades of experience, we have to admit those bean counters have been right. The problems have simply not been all that serious. Further, if we step back and take a sober look, it becomes clear those problems are still not all that serious.

All along, the constant refrain has been that we need to take security seriously and engineer our systems from the ground up to be truly secure. The recent report [3] opens with a quote from a 1970 publication (the well-known Ware Report) that called for such moves. This demand has been growing in stridency and has been increasingly echoed by higher levels of management and of political leadership. Yet in practice over the last few decades, we have seen just a gradual increase in resources devoted to cybersecurity. Action has been dominated by minor patches. No fundamental reengineering has taken place.

This essay argues that this "muddle-through" approach was not as foolish as is usually claimed and will continue to be the way we operate. Cyber infrastructure is becoming more important. Hence intensifying efforts to keep it sufficiently secure to let the world function is justified. But this process can continue to be gradual. There is no need to panic or make drastic changes, as the threats are manageable and not much different from those that we cope with in the physical realm.

This essay reviews from a very high level the main factors that have allowed the world to thrive in spite of the clear lack of solid cybersecurity. The main conclusion is that through incremental steps, we have in effect learned to adopt techniques from the physical world to compensate for the deficiencies of cyberspace. This conclusion is diametrically opposed to the heated rhetoric we observe in the popular media and to the unanimous opinions of the technical and professional literature. No claim is made that this process was optimal—just that it was "good enough." Further, if we consider the threats we face, we are likely to be able to continue operating in this way. But if we look at the situation realistically, and plan accordingly, we might:

- Enjoy greater peace of mind
- Produce better resource allocations

The analysis of this essay does lead to numerous contrarian ideas. In particular, many features of modern technologies such as "spaghetti code" or "security through obscurity" are almost universally denigrated, as they are substantial contributors to cyber insecurity. But while this is true, they are also important contributors to the imperfect but adequate levels of cybersecurity that we depend on. Although a widely cited mantra is that “complexity is the enemy of security,” just the opposite is true in the world we live in, where perfect security is impossible. Complexity is an essential element of the (imperfect) security we enjoy, as will be explained in more detail later. Hence one way to improve our security is to emphasize “spaghetti code” and “security through obscurity” explicitly and implement them in systematic and purposeful ways. In general, we should adopt the Dr. Strangelove approach, which is to stop worrying and learn to love the bomb.

In other words, not just accept that our systems will be insecure. Recognize that insecurity often arises in systematic ways and that some of those ways can be turned into defensive mechanisms. We do have many incremental ways to compensate, and we have to learn how to systematically deploy them, so as to live and prosper anyway. The key point is that, in cyberspace as well as in physical space, security is not the paramount goal by itself. Some degree of security is needed, but it is just a tool for achieving other social and economic goals.

Historically, for many observers, a serious reassessment of the traditional search for absolute security was provoked by Dan Geer’s 1998 post [1]. However, awareness of general risk issues, and growing perception that they were key, can be traced much further back to various research efforts in the 1980s and the founding of Peter Neumann’s RISKS Digest in 1985. No attempt is made here to trace this evolution of attitudes toward security. That is a nice large subject that is left for future historians to deal with. This essay considers only the current situation and likely evolution in the near future.

2 THE TECHNOLOGISTS’ SKEWED VIEW OF THE WORLD

The critics of the standard “business as usual” approach have been presenting to the public both a promise and a threat. The promise was that with enough resources and control over system development, truly secure information technologies systems would be built. The threat was that a gigantic disaster, a “digital Pearl Harbor,” would occur otherwise.

The promise of real security was hollow. If there is anything that we can now regard as solidly established, it is that we don’t know how to build secure systems of any real complexity. (There is another factor that is not discussed here, namely, that even if we could build truly secure systems, we probably could not live with them, as they would not accommodate the human desires for flexibility and ability to bend the rules. But that is a different issue not in the scope of this essay.) Serious bugs that pose major security risks are being found even in open-source software that has been around and in extensive use for years, as with the Heartbleed defect. And some insecurities, such as those revealed in the recent Meltdown and Spectre attacks, not only go back decades, but are deeply embedded in the basic architecture of modern digital processors. They cannot be eliminated easily, and we will have to live with them for many years. The most we can hope for is to mitigate their deleterious effects.

The mantra, called Linus’s law, that “given enough eyeballs, all bugs are shallow” has been convincingly shown to be fallacious. There are only relative degrees of security. Still, we have to remember that this has always been true with physical systems. Furthermore, in both the cyber and the physical realms, the main vulnerabilities reside in people. Those creatures are not amenable to reengineering and are only very slightly amenable to reasoning and education.

The threat of digital catastrophe has also turned out to be hollow. Sherlock Holmes noted that the “curious incident” in the Silver Blaze story was that the dog did not bark. In information technology insecurity, there are two curious “incidents” that have not attracted much notice:

- Why have there been no giant cybersecurity disasters?
- Why is the world in general doing as well as it is?

Skeptics might object and point out to any number of ransomware, identity theft, and other cybercrime cases. But those have to be kept in perspective, as is argued in more detail later. There have been many far larger disasters of the non-cyber kind, such as 9/11, Hurricane Sandy, the Fukushima nuclear reactor meltdown, and the 2008 financial crash and ensuing Great Recession. Has any cyber disaster inflicted anywhere near as much damage to any large population as Hurricane Maria did to Puerto Rico in 2017?

In the cyber realm itself, we have experienced many prominent disasters. But most of them, such as airlines being grounded for hours or days or cash machine networks not functioning, have arisen not from hostile action, but from ordinary run-of-the-mill programming bugs or human operational mistakes. And of course we have the myriad issues such as cost overruns and performance disappointments which plague information as well as other rapidly evolving technologies. They have little to do with the lack of cybersecurity. Yet we suffer from them every day.

There is a third curious incident in information technology (in)security that also appears to be universally ignored. For several decades we have had simple tools for strengthening security that did not require any fundamental reengineering of information systems. A very conspicuous example of such tools is two-factor authentication. The widely cited and widely accepted explanation for this technology not having been deployed more widely before is that users disliked the extra bother it involved. So apparently decision makers felt that the extra security provided by two-factor authentication did not warrant the cost of inconveniencing users. The big “dog did not bark” question then is, given that this technology was not deployed, why did nothing terrible happen?

The general conclusion of this essay is that from the start, the “bean counters” understood the basic issues better than the technologists, even though they usually did not articulate this well. The main problem all along was risk mitigation for the human world in which cyberspace played a relatively small role; it was not absolute security for the visionary cyberspace that technologists dreamed of.

3 THE STATE OF THE WORLD

One could object that the world is not doing well and point to climate change, rising inequality, civil wars, unemployment, and other phenomena that are cited as major ills of our society. But that has to be kept in perspective. Let’s put aside, until the next section, questions about issues such as long-term sustainability of our civilization. If we just look at where the human race is today from a long-term historical perspective, we find stunning advances by many measures, such as the number of people on Earth, how long they live, and how educated they are. There are more people today who are obese than hungry, which is unprecedented. Obesity is certainly not ideal, but can easily be argued to be an advance on the historically dominant feature of human lives.

Of course, there are a variety of threats for the future. But we need to remember that the progress that has occurred has relied often and in crucial ways on information systems that were, and are, insecure. Further, almost all of the most serious threats, to be considered next, are little affected by cybersecurity or lack of it.

4 THREATS

We certainly do face many threats. In particular, we do face many cyber threats. It seems inevitable that we will suffer a “digital Pearl Harbor.” What we have to keep in mind is that we have suffered a physical Pearl Harbor and other non-cyber disasters that large or larger. Many occurred quite recently, as noted before. It seems absolutely certain we will suffer many more, and an increasing number of them will surely be coming from the cyber realm. On the other hand, it is questionable whether the cyber threats are yet the most urgent ones.

The human race faces many potentially devastating non-cyber dangers, such as asteroid strikes, runaway global warming, and large pandemics. These threats could have giant impacts, but are hard to predict and quantify and are seemingly remote, so tend to be ignored by almost all people most of the time. However, we also face a variety of other still large dangers, such as those from earthquakes and hurricanes. Those occur more frequently, so the damage they cause is moderately predictable, at least in a long-run statistical sense. Yet we are not doing anywhere near as much to protect against them as we could, if we wanted to do so. We accept that they will occur and rely on general resilience and insurance, whether of the standard variety, or the implicit insurance of governments stepping in with rescue and recovery assistance.

We also tolerate the ongoing slaughter of over a million people each year in automobile accidents worldwide (with about 40,000 in the United States alone). The horrendous losses of human life as well as property that involve cars arise mostly from unintentional mistakes. They result from our accepting the limitations of *Homo sapiens* when dealing with a dangerous technology. It’s just that this technology has proven extremely attractive to our species. Hence we accept the collateral damage that results from its use, even though it far exceeds that from all wars and civil conflicts of recent times.

On top of accidents we also have the constant ongoing malicious damage, coming from crime in its many dimensions. Society suffers large losses all the time, and mitigates the threat, but has never been able to eliminate it. We have large security forces, criminal courts, jails, and so on. The United States alone has close to a million uniformed police officers and more than a million private security guards.

Military establishments tend to be substantially larger than law enforcement ones. The main justification for them is to guard against the far rarer but potentially more damaging actions of hostile nations. One way or another, most societies have decided to prioritize protection against those external dangers over that of internal crime. Further, in recent decades, military spending (and therefore total security-related spending) has been declining as a fraction of the world’s economic output. So when societies feel threatened enough, they do manage to put far more effort into security than is the case today.

Yet even military security at its very best is not watertight, which has to be kept in mind when considering cybersecurity. Serious gaps have been uncovered on numerous occasions, such as a deep penetration of an American nuclear weapons facility by a pacifist group that included an 82-year-old nun.

The bottom line is that society has always been devoting huge resources to security without ever achieving complete security. But those huge resources are still not as great as they could be. That’s because, as noted above, security is not the paramount goal by itself. We make trade-offs and are only willing to give up a fraction of the goods and services we produce for greater safety. There is even extensive evidence for human desire for a certain level of risk in their lives. When some safety measures are introduced, people compensate for that by behaving with less care.

Still, we do employ many people and extensive resources protecting ourselves from traditional physical world threats, far more than we devote to cybersecurity. Hence it is clear, and has been clear for a long time, that more effort could have been dedicated to cybersecurity, even without consuming productive resources. All we had to do was just shift some of the effort devoted to traditional physical security to the cyber realm. And indeed that is what is happening now, at least in relative sense. More attention and resources is being devoted to cybersecurity. One measure of the greater stress being placed on this area is the growing (but still very small) number of CEOs who have lost their jobs as result of security breaches. So the question arises, essentially the same question as before, just in a different form: Why was this not done before, and why has not much harm come from this?

5 HUMANSPACE VERSUS CYBERSPACE

It is very hard for technologists to give up the idea of absolute cybersecurity. Their mind-set is naturally attracted to the binary secure/insecure classification. They are also used to the idea of security being fragile. They are not used to thinking that even a sieve can hold water to an extent adequate for many purposes. The dominant mantra is that "a chain is only as strong as its weakest link." Yet that is probably not the appropriate metaphor. It is better to think of a net. Although it has many holes, it can often still perform adequately for either catching fish or limiting inflow of birds or insects. A tight sieve can even retain a substantial amount of water for a while.

Technologists also tend to think of information systems as isolated. This attitude is represented beautifully by the famous 1996 creation of John Perry Barlow: "A Declaration of the Independence of Cyberspace." This proclamation, which today seems outlandishly ludicrous, proclaimed the existence of a new realm, "cyberspace," that was divorced from the physical world and did not need or want traditional governments or other institutions. The key assumption was nicely formulated in the oft-quoted passage:

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

Indeed, if cyberspace were totally divorced from humanspace, and if all the "transactions, relationships, and thought itself" depended just on some mathematical relationships, then cybersecurity would be of paramount importance. An opponent utilizing a clever mathematical idea to break a public key system, or stealing a password, might wreak unlimited havoc.

And indeed, as the increasing number of incidents with bitcoin and other cryptocurrencies proves, such dangers do lurk in pure cyber realms. Further, they cannot be avoided. As was discussed before, people are incapable of building completely secure systems, they do choose weak passwords or leak strong ones, they do fall prey to phishing attacks, and every once in a while a mathematical breakthrough does demolish a cryptosystem.

What makes our lives tolerable is that the Barlow vision is divorced from reality. Cyberspace is intimately tied to what we might call humanspace, the convoluted world of physical objects and multiple relations, including institutions such as governments, and laws, and lawyers. In fact, we can say:

> The dream of people like Barlow was to build a cyberspace that would overcome the perceived defects of humanspace. In practice we have used the defensive mechanisms of humanspace to compensate for the defects of cyberspace.

Those defensive mechanisms are what we consider next, starting with the limitations of attackers in both physical and cyber realms.

6 PLUSES AND MINUSES OF NATURAL STUPIDITY

There are extensive discussions going on about the promises and threats of artificial intelligence (AI). Much less is said about natural stupidity and its positive aspects. Yet it is central to human life and key to enabling society to function. (At an even more basic level, the astounding level of human credulity, which enables so many attacks, is an essential element of human psychology and sociology and enables the cooperation that has led to modern civilization.) In particular, we are alive and living pretty well largely because most criminals are stupid.

This includes terrorists. Most of them are stupid, too. They are in almost all cases more like the Shoe Bomber than the highly trained and highly proficient professionals that the multitudes of publicly prominent cyber Cassandras hold out as big threats to our lives. Most crimes are extremely mundane, and many more could easily be solved if more effort was devoted to them. Criminals constantly make foolish mistakes, such as leaving their fingerprints, or their DNA, on the scene or driving their own cars. As a result, general crime has been kept within tolerable bounds for most of human history.

It is not just the most stupid people who make mistakes. Everyone does so. In fact, the mistakes of the smartest individuals are often the most disastrous, as they get entrusted with the most important jobs. Even the highly trained and highly proficient professionals in the military and intelligence agencies are fallible, including when at the peak of training and preparation. It is this fallibility that helps make cyberspace more similar to physical space than is commonly thought. Detecting where a network attack originates is harder than detecting where a ballistic missile is launched from. But digital forensics is a thriving field, largely because of human mistakes. Even the Stuxnet creators were not able to completely erase their "digital fingerprints," leading to high confidence as to their identities.

Cybercrimes not only leave digital fingerprints. They are usually tied in one way or another to the physical world, most frequently through flows of money. Hence there are far more ways to trace them than would be the case if they happened purely in cyberspace. Once tracing is possible, measures to deter, prevent, and punish can be brought to bear. Those digital fingerprints also mean that natural stupidity of attackers has more opportunities to display itself. And that offers opportunities for defense and countermeasures, just as in the traditional environment.

7 SMART AND STUPID CRIMINALS

The reasons most criminals are stupid are worth considering. An important one is that we mostly hear of the criminals who get caught and that is not a perfectly representative sample. The smart ones avoid detection and capture. But the really smart ones mostly figure out it is far safer and more comfortable to stay close to the line of legality. Serious damage to the system as a whole, or even to many individual players, tends to provoke strong countermeasures. Some criminals even learn to be symbiotes and contribute positively to society.

An insightful analogy can be drawn with biology. A virus that kills the host instantly tends to perish, as it has little chance to spread. The more successful viruses (more successful in terms of being widespread) are like those for the common cold, which cause relatively small annoyances that serve primarily to help them propagate. Many parasites evolve to become symbiotes, and the study of commensal relationships is a thriving field with a variety of examples.

8 THE CYBERCRIME ECOSYSTEM

Most criminals, even among those on the extreme edge of the stupidity spectrum, have no interest in destroying the system they are abusing. They just want to exploit it to extract value for themselves out of it.

An amusing and instructive example of illicit cyber behavior that maintains the functioning of the system is provided by the ransomware criminals. Studies have documented the high level of "customer care" they typically provide. They tend to give expert assistance to victims who do pay up and have difficulty restoring their computers to the original state. After all, those criminals do want to establish "reputations" that will induce future victims to believe that payment of the demanded ransom will give them back control of their system and enable them to go on with their lives and jobs.

An extreme example of exploitation of cyber insecurity without causing noticeable damage is that of national intelligence agencies. They carry out extensive penetrations of a variety of government and commercial systems, but are usually just after limited pieces of information and try (and usually succeed) in staying inconspicuous. In most cases they exploit only a tiny fraction of what they acquire, precisely in order not to raise suspicions about their activities. Of course, their activities do involve other dangers, when they acquire control of systems for future large-scale hostile activities. But such penetrations by state actors have to be handled at state levels, similarly to what occurs in the physical realm.

There are certainly some malicious actors who simply want to inflict damage, whether it is against a person against whom they have a grudge or, especially in case of terrorists, against society at large. But even such people are generally not as dangerous in cyberspace as they could be. First of all, there are not that many of them. Second, they generally have limited skills and resources, and are mostly very foolish, and engage in foolish activities. The more rational among them choose their targets and methods for maximal effectiveness in achieving whatever nefarious purposes they have in mind. For terrorists, say, cyberspace is generally not very attractive as a target. Blocking people from withdrawing money from cash machines or even causing a blackout in a city does not carry as strong a message as blowing up airplanes, bringing down buildings, or causing blood to flow among spectators in a sports arena.

There is much concern about ongoing technology developments making the lack of cybersecurity far more dangerous, especially as more devices go online and IoT (the Internet of Things) becomes more pervasive. Those are valid concerns, but let us keep in mind that those ongoing technology developments are also creating or magnifying many physical dangers even without taking advantage of cyber insecurity. Just think of drones (or possibly imaginary drone sightings) shutting down airports recently or drones or self-driving cars delivering bombs in the future.

In general, and reinforcing earlier discussions, society has always faced manifold dangers from its members misusing various technologies. Deterrence, detection, or punishment, in addition to general social norms, is what has enable civilized human life to exist. Contrary to the cyberlibertarian visions of people like Barlow (or many modern advocates of bitcoin and blockchain), they are likely to be just as crucial in the future, if not more so.

Of course, as the old saying goes, bank robbers went after banks because that is where the money was. But now the money is in cyberspace. So that is where criminals are moving. And that is also where security resources are being redirected, completely natural and expected, and happening at a measured pace.

9 BLACK SWANS VERSUS LONG TAILS

Cybersecurity efforts are dominated by very mundane work, monitoring the automated probes of the network or attacks of the "script kiddies." And perhaps most prominent and most boring, but absolutely critical, is assisting legitimate users who have forgotten their passwords, which is exactly analogous to the state of traditional physical security. Much of the time of firefighters and police officers is devoted to rescuing kittens stuck high up trees or handling temporarily inebriated but otherwise perfectly respectable citizens.

The evolution of the cybersecurity field over the last few decades has led to wide recognition among its practitioners that threats cannot be entirely eliminated. There are frequent references to minimizing "the attack surface," for example. This reflects the reality that one can limit attacks and the damage they can do, but not get rid of them. More resources can be used to lessen threats. But those resources are costly, either in terms of the pay and equipment of the security professionals, or, what is typically much more important, in terms of constraints on the legitimate users. So one is led to look at optimizing the allocation of resources and studying and modifying the incentives. One outgrowth of such thinking on the academic side has been the rise of the field of economics of information security. It has produced a flourishing literature and a series of annual workshops. Together with all other academic and industry efforts, it fits into the basic philosophy that animates modern economics, namely, of studying systems in equilibrium. There is ongoing hostile activity that is counteracted by security measures, and the task is to select the optimal combination of those measures that fit within some budget constraints.

One could view such approaches as concentration on the "long tail" of security threats. There are many of them—they require large resources in the aggregate to deal with, but individually they pose limited and reasonably well understood dangers. Overall, their potential impact can be estimated and constrained by standard approaches.

But then, at the other end of the spectrum, there are the "black swans," the giant security breaches that cause major damage. Those don't fit into the equilibrium framework (just as catastrophic financial collapses don't fit into the standard economic equilibrium framework and have been almost entirely ignored by mainstream economists). But neither do the giant physical disasters, such as Pearl Harbor or Hurricane Katrina. Their damaging effects basically can only be mitigated by designing in general resilience.

Measures that provide resilience against cyber attacks are often the same as those against traditional physical attacks or against natural disasters. As just one example, there is much concern about the damage to the electric power grid that might be caused by malicious actors. But the worst scenarios along those lines are similar to what we are sure to suffer when something like the Carrington Event occurs. This was the giant geomagnetic solar storm that hit the Earth in 1859. It caused widespread failures of the telegraphs, the only electrical grids in existence at that time. Estimates are that if it were to recur today, it would cause damages in the trillions of dollars. And it is bound to recur some day!

The conclusion that emerges is again that cyberspace is not all that different from the more traditional physical space we are more used to. And security measures for the two are again similar.

10 NEGLECT OF OBVIOUS SECURITY MEASURES

The main thesis of this note—that cybersecurity is not very important—is illustrated nicely by the phenomenon of two-factor authentication. This technique is spreading. It is not a panacea, but there is general agreement that it offers significant enhancement to security.

But why is it only now that two-factor authentication is coming into widespread use? The basic technique is ancient by the standards of the information technology industry. Two and a half decades ago, it was used at my employer of that time. The hardware tokens came from one of several suppliers that were already in that line of business.

Yet even at my former employer, two-factor authentication was abandoned after a while, and in most places, it was never put into service in that era. So what has changed to finally make this technology used more widely? As often happens, it was likely a combination of factors:

- Threats have increased.
- Implementing two-factor authentication has become easier.

The old hardware tokens of the 1990s were not very expensive, but they had to be carried around (as opposed to receiving a text on a mobile phone that people have with them almost all the time, say), and they required typing in strings of arbitrary symbols. Now we can use short texts, or hardware tokens that plug into a computer, or else mobile phones that communicate with a nearby computer wirelessly. So while the monetary costs of the basic system have not changed dramatically, the costs to users have declined significantly. And, of course, the threats have increased, as noted above, so the incentives to use two-factor authentication have grown.

Yet even now, two-factor authentication is nowhere near universal. Further, most deployments of it at this time appear to use the least secure version of it, with texts to mobile phones. Practical attacks on this version have been developed and applied. The more secure versions with hardware tokens are used much less frequently. Obviously what is happening is that choices are being made, the additional inconvenience to users being weighed against the likely losses from hostile penetrations. Even without any new technology breakthroughs, more secure versions of two-factor authentication can be deployed when they are seen as necessary. But they are clearly not being seen as necessary at present.

There are many more examples of relatively easy steps that have been available for a long time and can strengthen security without any fundamental reengineering of information systems or rearranging how society functions. Consider the adoption of chip credit cards. They have been universal in much of the world for years, but are only now taking over in the United States. The costs have been understood by the banking industry, and it was decided, through a messy process by various stakeholders, that they were too high until the perceived threats increased.

Electronic voting is another prominent example where simple and well-known steps would have provided greater security a long time ago. Experts have been arguing from the start that purely electronic voting basically cannot be made secure, at least not with feasible technology and the financial resources that are available or are likely to be made available. All the evidence that has been gathered over the years supports this view. Further, all the advantages of electronic voting (convenience, accessibility for those with handicaps, quick collection of results, etc.) can be obtained very easily, together with a much higher degree of security, through the use of printed records that are preserved in physical form. The additional costs that are involved are very modest and seem well worth it to most people who have examined the situation, including this author. Yet in many jurisdictions this simple solution is being ignored. And it has to be admitted that so far no serious abuses have been documented. What is likely to happen is that if some big scandal surfaces that is based on a cyber breach, political leaders will swing into action and find the resources to provide the obvious solution. (We should remember that big voting scandals do occur all the time, based on other aspects of the voting system, and they lead to responses that vary with circumstances.) But, as seems typical in human affairs, it will likely take a big scandal to cause this to happen.

Electronic voting provides an interesting illustration of a cyber insecurity that is not difficult to fix, but is not being fixed. It also provides an example of a common phenomenon, namely, that the fix involves stepping back to the traditional physical world, in this case of messy paper ballots. (The same could be said of chip cards.) In other words, the insecurity of the cyber realm is compensated by a measure from the brick-and-mortar world.

An even better example of reliance on physical world to compensate for defects in cybersecurity is that of passwords. They have been pronounced obsolete and dead many times, but are still ubiquitous. A key element in making them more tolerable in spite of their well-known weaknesses is the use of paper for users to write them down (or, preferably, to write down hints for those passwords or passphrases). The security field has finally been forced to admit that asking users to remember scores of complicated passwords (and change them every few months) is not going to work, not with the bulk of human users. But paper slips work out quite well, as physical wallets and purses do not get stolen all that often.

Notice that there are many other direct physical methods for increasing security. Air-gapped systems, isolated from the Internet, have been standard in high-security environments. They are again not absolutely secure, as the Stuxnet case demonstrates. But they do provide very high levels of security, as breaching them requires special skills and extensive effort (as the Stuxnet case demonstrates, again). At a simpler level, allowing certain operations (such as resetting the options on a router or another device) only through the press of a physical button on the device also limits what attackers can do.

Frequent backups serve to mitigate ransomware and many other attacks. They can be automated so that they do not impose any significant mental transaction costs on the users. They increase the reversibility of actions, which is a key component to security (but seems not to be understood by the advocates of bitcoin and other cryptocurrencies). And they are not expensive in terms of hardware. Of course, backups increase security only if they are not subverted. But there are a variety of ways to make backups more trustworthy, such as using write-only media (such as some optical disks) or special controllers that limit what operations can be done.

We should also remember there is one piece of advice that applies in both cyberspace and physical space: if it's dangerous, don't use it! Some very cautious organizations disable USB ports on their computers, but such organizations are rare. Email attachments are a notorious carrier for all sorts of malicious software. They could be blocked, but seldom are. All these examples show how society has in effect accepted obvious risks in order to get benefits of insecure information technology solutions.

11 SURVEILLANCE CAPITALISM AND LOSS OF PRIVACY

The analogy between cyber and physical security is strong, but there are certainly substantial differences. The one that appears to be cited most frequently is privacy. There was no absolute privacy in the past. In particular, there was always the most intractable problem of all, namely, that of insider disclosure. (According to an old saying, "two people can keep a secret, as long as one of them is dead.") But modern threats to privacy are orders of magnitude larger than those faced in the past. Further, as we move forward, our central and giant problem is that potential leakers are proliferating at a rapid pace. Individuals can convey far more information now than in the past, as the Manning, Martin, and Snowden information torrents from NSA demonstrate. For the majority of people, though, the main threat comes in the shape of the many devices we use, which is increasing in numbers and in their capability to transmit information about us to others. The cell phone is the premier example, but increasingly so is our fitness tracker, our TV set, and our electric meter. Practically nothing that we will be doing can be assumed to be secret in the future. This will even apply to our physiological reactions, even ones we do not express, or may not consciously be aware of, since they might be discerned by various sensors.

Already today, the old mantra that "on the Internet, nobody knows you are a dog" has in practice been turned on its head. Many organizations know not only that you are a dog but also what breed of dog you are and what kind of fleas you have.

For the purposes of this essay, the key counterpoint to this line of argument is that this erosion of privacy we experience has little to do with cyber insecurity. Some of that erosion does come from illicit hacking of our systems, which is indeed facilitated by the insecurity of our information systems. But most of it comes by design, as providers of services and devices purposely build them to collect data about users for exploitation by those providers and their (almost universally concealed) networks of partners. (Even the illicit hacking of those devices, databases, and so on can occur only because of this huge and legal, even though usually obfuscated, data gathering.) Hence there are no improvements in cybersecurity that would by themselves make a measurable difference to the erosion of privacy that we experience. To the extent that society wants to preserve some semblance of privacy, other methods will have to be used, which likely will have to be based on laws and regulations and to some extent on technologies for users to protect themselves.

On the other hand, the erosion of privacy is a key element to maintaining tolerable levels of security in general. Tens or sometimes hundreds of millions of credit cards are routinely captured by criminals by compromises of databases. Yet the overall damages are limited and often dominated by the cost of arranging for replacement cards. The prices of stolen credit card credentials on the black market are low, on the order of a dollar or so each. The reason is that banks have developed techniques for detecting credit card fraud. Those are based on knowledge of users' patterns of behavior. A typical card holder is not an anonymous "standing wave" of Barlow's imagination, or some account even more anonymous than those involved in the not-all-that anonymous bitcoin operations. Instead, such a person is in most case an individual who mostly follows a staid routine in life and in commercial transactions, say, stopping by a particular coffee shop on the way to work or dropping in at a grocery store on the way back from work.

There are many measures that erode privacy, such as cross-device tracking (in which users are identified even though they use different gadgets) or identifying users by the patterns of their typing, that are often regarded as objectionable or even creepy. Yet they do serve to identify users, and thereby to prevent mischief, even if this is incidental to the main purposes for which they are deployed. Organizations that operate these systems can get a high degree of assurance as to the person they are dealing with and in such circumstances stealing a credit card or cracking a password is often of limited use.

It should also be remembered that since enterprises do want to track customers or potential customers for their own business reasons, they have incentives to develop and deploy those privacy-invasive methods in preference to providing more direct security. This is a case where general economic incentives skew what security methods are used. But those methods are very effective in compensating for cyber insecurity.

12 THE DECEPTIVELY TRANSPARENT BUT OPAQUE WORLD

The development of information technology does mean that nothing can be assured of staying secret. (The Manning, Martin, and Snowden security breaches at NSA cited above are only some of the most prominent examples.) There are just too many vulnerabilities in our systems and too many tools to capture and extract information, such as cameras in our cell phones and miniature cameras that are getting ever smaller and harder to detect. But neither can it be assumed that all relevant information will be available in forms that lead to action. The technique of "hiding in plain sight" was popularized by Edgar Allan Poe two centuries ago. Modern technology creates so much more information that this often works with minimal efforts at concealment, or even without any such effort. Even when information is known, it is often not known widely and is not known by people who might or should act on it. Just consider Dieselgate, where various groups had obtained measurements of emissions exceeding legal limits years before the scandal erupted. Or think of the Danish bank that laundered over $200 billion through a small Estonian branch over a few years—not to mention all the various sexual harassment cases that took ages to be noticed publicly.

In general, information that can be captured by information systems is becoming more detailed and far more extensive. But it is still limited in many ways. One of the most important ones is that human society is a messy affair and much that goes on is hard to codify precisely. In particular, tacit knowledge is crucial for individuals and organizations. Hence