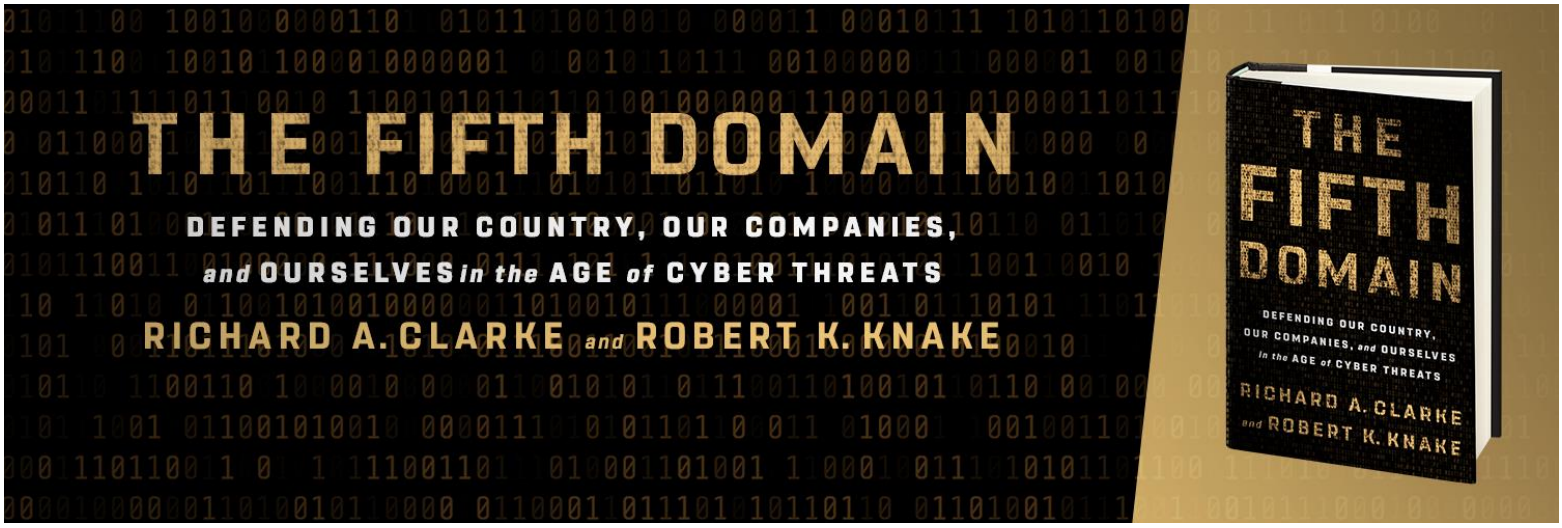
The Fifth Domain — Excerpt



Chapter 1 The Back of the Beast

The future is already here; it's just not very evenly distributed.

—William Gibson

Sitting in the back of the Beast, the armored vehicle custom made for the President of the United States, Bill Clinton wanted to talk about his cousin from Hope, Arkansas. He didn't want to talk about the major speech he was about to give at the National Academy of Sciences. It was January 1999, and Clinton had just proposed budget initiatives to com- bat emerging threats, including those in the cyber domain. Few people then saw cyber threats as a major problem. But he did. Dick Clarke sat next to him with a PowerPoint deck and an annotated version of the speech, but the President was channeling his Bubba persona, telling a story about Arkansas, and not to be stopped.

When the Beast pulled into the underground parking at the academy, Clinton finally turned to the business at hand. "I read the speech. It's okay." That meant it wasn't.

"But really, isn't what we want to say something like this: Throughout history there is a competition between offensive and defensive technologies and a gap between their development. A guy in a cave carves a rock and at- taches it to a stick and creates a spear, and then someone needs to defend against that, so they get some animal hides and make a shield. Later on, people defend towns with walls and then some guy invents battering rams and catapults. But there is time between when an offensive weapon is created and when the defensive counter to it comes along." A Secret Service agent standing next to the vehicle opened the heavy door of the Beast. You cannot really open it from inside.

The President kept going, warming to his theme. "And right now, the problem is that the new offensive technologies have taken to the field and they now have the advantage over the things that we

have to defend against them. So, what we have to do is invest in new technologies that will give the defense an advantage again, or at least even out the playing field. Have I got that right?"

Clarke looked at the President, bemused, reminded again about the preternatural ability he had to make the complex comprehensible. Clarke put away his copy of the draft speech and the PowerPoint deck, sighed, and said, "Yeah Mr. President, you should say that today." And he did.

Nineteen years and three months later, Clinton said the same thing verbatim in answering a question about his cyber-oriented novel while sitting on stage in Washington's Warner Theatre. It was still true. In the intervening twenty years, hundreds of billions of dollars in public and private investment in cybersecurity research, development, and deployment had not fundamentally changed the advantage. It remains a case of what military theorists call offensive advantage or offensive preference.

Offensive Preference in Cyberspace

Any scenario between adversaries is a balance between offense and defense. When the offense has the advantage because of some combination of technological superiority or cost, military theorists write, there will be conflict. When the reverse is true, when it costs more to attack, or when the chances of an attack defeating the defenses is low, greater stability will prevail. We think these generalities apply now to the ongoing hostilities between hackers and corporations, to the current covert espionage done by nation-states, and to the potential for a future nation-state-on-nation-state cyber war. Today, as for the last twenty-five years, the conventional wisdom in the fields of computer science, information technology, and networking is that there is an enormous offensive preference. That might not have been a big deal to most people, except that in the last twenty-five years, we have also made almost everything dependent upon computer networks. In fact, be- cause the offense is thought to have the advantage right now, in a crisis situation of possible conventional warfare, there is likely to be an inclination to go first with a cyberattack.

This book is about how the balance between offense and defense is changing and how the rate of change can be increased to set us on the path to stability. We think it is possible to reduce the risks posed by offensive cyber technologies and actors, and to increase peacetime stability for corporations and crisis stability for nations.

As we write this is 2019, we see a pattern of malicious activity in cyberspace that suggests we are already engaged in a low-grade, simmering cyber conflict with Russia, China, and Iran. We also are beginning to turn a corner on this problem. Estimates put worldwide cybersecurity spending at $114 billion in 2018. Venture capital investment in cybersecurity technology is up, topping $5 billion in 2018 alone. More than three thousand new technology firms have sprung up, backed by ample venture capital, to develop new solutions. Cyber insurance was long a fringe product. Today, the market is (finally) growing and thriving, with almost $2 billion in premiums written in 2017.

Long-standing problems created by government, such as barriers to information sharing, have been solved and companies are actually beginning to organize communities not only to share information, but also to provide mutual aid during crises. One chief information security officer (CISO) at a major bank we spoke with thinks that in five years his bank will largely be immune to cyberattacks as it upgrades from legacy systems that are inherently insecure to systems that are secure by design. Many leaders in Silicon Valley, where optimism is never in short supply, would tend to agree.

Today, if you are a small-business owner, you can conduct most of your work online and do so with the support of cloud service providers that have dedicated thousands of people and billions of dollars to protecting your data. Automation and artificial intelligence have the potential to erase much of the attacker's advantage. Yet, at the same time, attackers are looking at how they can use these tools as well. Quantum computing could provide both impossible-to-break protection for data and the ability to crack all current forms of encryption. Blockchain, which many technologists think could lead to fundamentally more secure protection of data, has for the time being found its biggest use in cryptocurrency, a technology that is decidedly giving an advantage to attackers by allowing criminals to move their ill-gotten gains around anonymously. These technology trends could shift the balance in either direction. It is up to us to determine which way the scales will tip.

The Pentagon has long identified four primary domains of conflict: land, sea, air, and space. In recent years, cyberspace has come to be known as the "fifth domain." Unlike the others, cyberspace is man-made. It can therefore be changed by man. It is a positive attribute of cyberspace that once a weapon has been used and discovered it can be blocked. That is the equivalent of changing the atmosphere so that bombs can no longer fall.

We have been working together on the cyber problem for fifteen years. We both consult for major corporations, cybersecurity companies, and venture-capital and private-equity firms. We have both been adjunct faculty members teaching graduate students about cybersecurity. And, for our sins, we have both spent time in government agencies, Dick Clarke in the Defense Department and State Department, Rob Knake in Homeland Security. The best parts of our government experiences, however, were in the White House, on the National Security Council staff. Dick served on the George H. W. Bush (41), Bill Clinton (42), and George W. Bush (43) staffs. Rob served on the Obama staff (44).

While in the White House, we both had the opportunity to author decision documents (executive orders, presidential directives) on cyber- security. Dick also drafted the first national strategy on cybersecurity that any nation ever published. So, yes, you can blame us in part for some of the mess, but we think we also have some unique perspectives. Between us we have spent more than four decades closely following the evolution of the cyber threat and the government and corporate response. Ten years ago, when we wrote the book Cyber War: The Next Threat to National Security and What to Do About It, our goal was to raise the alarm. We knew the seriousness with which cyber threats were taken in Washington, but didn't see the same level of concern in the private sector. Unfortunately, much of what we wrote about cyber threats turned out to be right, but things have also changed a lot since then, including our prescriptions.

When we wrote Cyber War, Silicon Valley, still stuck in its "Don't Be Evil" phase, wouldn't accept that its inventions had the potential to cause real harm. Our intention was to scare government and corporate leaders into addressing the threat before the prospect of cyber war turned into a real cyber war. In the intervening decade, far too little has happened to respond to the threat, while many of our predictions on the emergence of war in cyberspace have regrettably come true. Yet cybersecurity remains a solvable problem, one far less difficult to address than a host of others, like climate change, that we face today.

We have full faith that, in time, we will find workable solutions to the problems that plague cyberspace today through an ugly and disruptive process of trial and error. Eventually, businesses will come around to recognizing the value they get from being globally connected and will start investing appropriately to secure that value. Eventually, governments will figure out their roles and begin to help the private sector help itself.

But unless we are smart and proactive, we will solve the challenges we face in cyberspace only after multiple crises. After cyberattacks cause blackouts in the United States, we will make the necessary investments to prevent them. After train derailments, ship collisions, or airplane crashes caused by malicious actors operating in cyberspace kill people, we will build systems that have near-zero tolerance for failures caused by hackers.

The danger is that, after events like these, we won't just do the hard work of making our systems resilient to cyberattacks. Blood will need to be answered with blood. We think it safe to conclude that the next major war the United States enters will be provoked by a cyberattack. That provocation may be accidental. It may be intentional. But the United States does not have a good record of turning the other cheek. And so as we think about what needs to be done to improve cybersecurity, our fundamental goal is to achieve cyber peace so that we do not end up embroiled in more devastating and costly wars in the real world.

Our collective understanding of these problems as a community of practitioners has grown immensely in recent years. We now have a clear view of the many problems that make cyberspace an attractive domain for war- fighters, and of how we could make it less attractive. As we developed the concept for this book, we kept coming back to the realization that the specter of cyber warfare does not overshadow all the good things that are made possible by the internet. The speed and connectivity that enable cyber warfare also enable email, social media, Amazon Prime, and massive multiplayer games. While some might question whether these applications represent positive outcomes for society, this global network has allowed collaboration and communication that was undreamed of a few decades ago and has been the driving force behind massive increases in productivity and wealth creation.

By some estimates, the digital economy, separate and apart from the traditional economy, is growing at three times the rate of the rest of the economy. But as the global consulting firm McKinsey points out, it's increasingly difficult to separate the digital economy from the rest, as every company today is wired up. McKinsey estimates that fully 98 percent of the economy is being impacted by digitization. It is no coincidence then that the companies thriving today are the ones that have taken cybersecurity seriously. In 2018, we saw the first real hits to companies' bottom lines from cyberattacks. The NotPetya malware took billions from companies operating in Ukraine, Europe, and the United States, leading many to report the losses on their quarterly and annual filings with the Securities and Ex- change Commission. Yet some, if not most, multinational corporations operating in Ukraine either were not impacted, were minimally impacted, or had some really good lawyers who argued the losses did not need to be reported (more on that later).

Companies such as Microsoft, Apple, and Google, all companies that at one time saw concerns over cyber threats as overhyped, now have religion and are investing in cybersecurity with the zealotry of the converted. They view cybersecurity as a competitive advantage in a market where consumers are increasingly wary of doing business online. Large banks such as Citi, Bank of America, and JPMorgan Chase also view cybersecurity as a competitive differentiator for both consumer and commercial clients.

The near daily press reports of new incidents and the constant stream of notifications that your personal information has been stolen have created the impression that cyberspace is hopelessly insecure. Yet hiding in plain sight are many examples of companies with big targets on their backs that have been able to constantly defeat even the best nation-state offensive teams year in and year out. While these companies have massive security teams and budgets in the hundreds of millions of dollars, their innovations, many borrowed from the military, are slowly making their way to the wider market.

The offensive advantage in cyberspace is slowly shifting as the defense closes the gap by taking advantage of new technologies, becomes better organized, and begins to understand the value of what is at stake. Accelerating that shift is one of the central requirements for achieving something more like peace and less like war in cyberspace.

Cyber warfare must become both more difficult and costlier to carry out. Cyber criminals, who act as proxies for nation-states as well as cause significant harm with their moneymaking schemes, must have their numbers culled. The barriers to entry for engaging in malicious activity in cyberspace have been going down steadily, year over year. They must be brought back up.

Many who have looked at the specter of cyber war have called for drastic action. "Reinvent the internet" to make it more secure is an often-heard refrain, but no one has yet come up with a plan for how to do that without causing more economic and social harm than the bad actors could do on their worst days. Even sillier are the calls for a "cyber Manhattan Project" or "cyber moon shot." These demands for a massive national effort always lack the same thing: a clear goal.

The Manhattan Project of the 1940s took developing theories of physics, as laid out in a succinct letter from Albert Einstein to President Franklin Roosevelt, and set out an engineering challenge to translate them into an atomic weapon. Kennedy's goal of the "moon shot" was even clearer: get to the moon. Cyber war has no such neat solution, because achieving peace in cyberspace is not a question of solving an engineering problem or reaching a specific location.

Some of the challenges blocking the way to cyber peace are technical, but most, at their heart, are economic. With the right package of economic incentives, the technical problems can be solved. So, while this book will dive into the 1s and 0s to explain the challenge, most of the solutions will be about how to make markets and governments work in the interest of promoting security. Above all, our guiding principle is to avoid solutions that would cause more disruption than the problems they are meant to solve. In cyber-space, this appears to be an easy trap.

The worst example of this tendency came at the end of the Obama administration, when officials at the Department of Justice proposed that companies should weaken encryption to make digital information readily accessible to law enforcement and also, therefore, to criminals. They failed, but many similar ideas are still being put on the table. When things go wrong in cyberspace, such ideas are likely to be introduced and reintroduced and will eventually be implemented if we do not, as a community, develop compelling alternatives.

Above all, as we seek solutions in this space, we are looking for rapid evolution, not revolution. We think there are enough companies that have figured out how to manage the threat that the challenge now is to create the right package of incentives to spread these models and to innovate faster than attackers can. As the cyberpunk author William Gibson said, "The future is already here; it's just not very evenly distributed." In a sense, therefore, the task at hand is to figure out how to more evenly distribute a secure cyber future.

A Different Threat, a Different Model

As we looked for solutions to problems that have long plagued cyberspace, what has not changed is our fundamental premise that cybersecurity is a shared responsibility between government and the private sector, with the onus for protecting computer systems falling on the owners and operators of those systems.

Dick first made the concept of a "public-private partnership" for cybersecurity official U.S. policy with Presidential Decision Directive 63 (PDD 63, for those in the know) in 1998. That directive also put in place many of the building blocks for realizing this vision that we still rely on today, such as information sharing and analysis centers (ISACs). Since then, across the Bush, Obama, and Trump administrations, specific policies have been rescinded and rewritten, but the overall thrust of U.S. cyber policy has remained largely unchanged. This degree of continuity across twenty years and four presidential administrations would be remarkable in any other area of public policy. At a time when Republicans and Democrats are sharply divided over climate change, immigration policy, and tax policy (to name a few), it is even more remarkable.

Since the Clinton administration, our cyber strategy has changed very little despite many attempts to come up with a different one. Thus, when we consider how to secure privately owned and operated networks, we return to the basic idea that the companies that own and operate the internet and the things that are connected to it, be they multinational media companies, providers of essential services, or the makers of the tiniest IoT devices, will be responsible for protecting themselves. They will do it through network defense, not offense.

Government's role will be limited, to support the private victims of cyberattacks with law enforcement, information sharing, diplomacy, and, in the rare cases where it is both feasible and in the national security interest, military force. Government will also play a role in helping the private sector help itself, through nudges to encourage investment and cooperation in cyber- security; through research, training, convening; and, ultimately, through regulation.

Despite twenty years of continuity on this policy, this division of responsibility is often derided in corporate America. Many CEOs are incredulous that they are responsible for defending their companies against foreign adversaries of the United States. "That's what I pay taxes for," echoes out of every boardroom. Leaders in national security often have the same view, believing that it is the responsibility of the U.S. military to defend the nation in cyberspace. They want to equate cyberattacks to nuclear missiles, and argue that it must be the government's role to stop these attacks.

The idea that government should find some magic way to make this problem go away and let us go about our business online is compelling to many. It's also deeply flawed. The cyber domain is fundamentally different from the air domain, as are the threats that lurk within it. Making cyber- security the military's responsibility would require rearchitecting the inter- net to give defense agencies the necessary choke points to try to filter out hostile threats. Doing so would require also granting them unlimited access to the content of traffic, a spy's dream and a privacy advocate's nightmare. Such an approach would likely still fail, and fail while incurring massive costs with tremendous societal disruption.

When cyberattacks do occur, every CEO would like to view it as a national security crisis, shift responsibility to government, and have the military "fire off the missiles." The desire to counterpunch is understandable, but foolhardy. Thus far, the U.S. government has shown remarkable restraint, avoiding engaging in reckless counterstrikes that would broaden conflicts. Whether that restraint will hold we do not know, but we are fairly certain that the utility of such strikes will be low.

Attribution (determining who is behind an attack) is a recurring challenge in responding to such attacks. Advanced threat actors have learned how to keep their computer systems hidden and are able to quickly replace any lost resources with other, likely stolen, computing resources, or make it appear as if another group altogether were responsible for an attack. Thus, counteroffense is at best like firing a cruise missile into an empty tent, and at worst like firing a cruise missile into a civilian apartment complex. And of course, along with relying more on the military, we must also take a dim view of vigilantism in

cyberspace, and hope that we will soon see the Department of Justice indict someone for so-called hacking back.

Late in the Obama administration, the government finally got out of the business of operating the last government-managed portion of internet infrastructure, the Domain Name System. With that function now firmly implanted in the private, nonprofit Internet Corporation for Assigned Names and Numbers (ICANN), the federal government has finally completed the internet's thirty-year transition from a science experiment at DARPA (the Defense Department's Advanced Research Projects Agency) to a wholly commercial venture. We spent thirty years getting the government out of operating the internet; we would not want security to be the reason we let the government back in.

What that leaves us with is the approach we have advocated all along: building systems so that most attacks cause no harm, and that allow us to respond to and recover from attacks that do succeed, with minimal to no disruption. We have adopted a different way to talk about this concept: cyber resilience. We also have ideas to share on how it can be implemented.

Cyber Resilience

The best strategies can be summed up with a single word. In the Cold War, we had two such strategies: containment and deterrence. George Kennan's famous "long telegram" took a few thousand words to spell out the strategy of containment, of keeping the Soviet sphere of influence limited. Thousands of papers and books would ultimately be written on deterrence in the nuclear era (and rewritten for the cyber era), but those single-word strategies clued everyone in to the basic ideas. Once set out in the 1940s, they held for almost fifty years with very little variation as times and presidential administrations changed.

Throughout this book, we will come back many times to the theme of working to shift the advantage from the attacker to the defender. This effort should be the overall goal of our national policy, and that of like- minded countries and companies. It's the right idea, but the language of offense-defense theory too readily suggests that cybersecurity is just an- other problem, such as terrorism or nuclear threats, that the military will deal with.

The reality of the internet as we know and love it today does not lend itself completely to traditional national security approaches. One of the guiding lessons we kept in mind while writing this book was the need to look for solutions by analogy that were not drawn from the world of warfare. This may seem rich, coming from the guys whose last book was titled Cyber War, but we believe that if the goal we want to achieve is cyber peace, then we should be looking at solutions to problems outside the fifth domain or any of the other four. If we try to find allegories in the Barbary pirates, or the battle of Fallujah, or the response to 9/11, we will no doubt find them, but they will lead us to one type of solution. Instead, throughout this book we have looked to other areas of study, such as ecology, public health, emergency management, and even psychology. As we have done that, one central theme continued to emerge: resilience. At the corporate level, many leaders are recognizing that their enterprise cybersecurity strategies need to be built around resilience. They must try to prevent every incident they can, but respond and recover rapidly when prevention fails. In his book Digital Resilience, RedSeal CEO Ray Rothrock identifies the concept of resilience as "a winning strategy in a losing war," arguing that the threat from cyber ac- tors has made resilience "table stakes for any enterprise interested in survival." Yet while the corporate world is starting to embrace resilience, many in Washington provide only lip service to the concept. Programs and bud- gets suggest cyber policy is stuck in a war-fighting mentality.

If you do a keyword search on cybersecurity strategies from the last few administrations, you will no doubt find the word "resilience" buried somewhere in the document. But the idea has never been

embraced as the central goal of our strategy. It has always been an ill-defined and vague concept. Ultimately, what we want is to be able to ignore cyberattacks, to be able to slough them off and continue on with our business rather than being forced to escalate. Because we insist on finding Cold War parallels, the cyber com- munity often talks about this concept as "deterrence by denial," the idea that we want to make our defenses so good that adversaries will not even try to attack, and if they do attack, it won't be of consequence. We'd propose a slight shift. We want to make our defenses so good, and our architectures so strong, that we do not care about whether we are being attacked most of the time because the attacks have no serious effects.

Cyber resilience must be built upon, rather than be seen as a replacement for sound security fundamentals. When confidentiality, integrity, and availability are compromised, resilience is about the ability to rapidly respond, return to a good state, manage bad outcomes, and learn from the incident so that future incidents are less likely. Here, it is important to note that thinking of "resilience" as the ability to recover to a previous state or to bounce back is too limiting. For resilience to be a useful concept in the field of cybersecurity, it requires that the concept fully embody the idea of re- turning stronger or better than before.

In the field of psychology, where the concept of resilience has been more fully developed than in any of the other fields that use the term, there is a built-in acknowledgment that resilience is not about returning to a previous state after an individual experiences trauma, but about adapting to that trauma. After the death of a spouse or parent or a child, after the loss of a limb or the trauma of war, overcoming these experiences does not mean forgetting them or getting back to the way you were before the experience. No one could.

Applying this psychological reality to the physical world, Judith Rohin, a psychologist by training and the former head of the Rockefeller Foundation, formulates a definition that works equally well for coping with cyber threats as it does for, say building resilient cities. Rodin defines resilience as the capacity of any "entity . . . to prepare for disruptions, to recover from shocks and stresses, and to adapt and grow from a disruptive experience." We think that definition transfers aptly to the cyber world.

In the next chapter, we provide a reminder of the threat and the damage that can be done. Then we look at corporations and the progress some of them are making at safeguarding their networks. We examine the potential for improved public-private partnerships and the role of regulation. We ask what the government and the military should do, and we examine the role of the international community. Because cyberspace is ever changing, we then discuss the new technologies and what they could mean for the offense- defense struggle. Finally, we have some suggestions about what you should do at home to secure your corner of cyberspace.

Throughout the book, we will try to show that we have a choice to make about the future we want in cyberspace. In the chapters that follow, we will sketch out why raising the alarm on cyber threats is warranted, and will lay out a plan for how the worst outcomes can be avoided. There are two futures we can choose from. It is up to us to decide which one we want cyberspace to become.

Chapter 2 EternalBlue, Eternal War

The Russian military launched the most destructive and costly cyberattack in history. . . . This was also a reckless and indiscriminate cyberattack that will be met with international consequences.

—Statement from the press secretary of the White House, February 2018

Lorina Nash rushed her mother to the emergency room at Lister Hospital in Stevenage, England. The doctors said they needed tests to diagnose the problem. They gave Nash's mother a blood test, but then the computers crashed and they could not complete the analysis. The doctors put the sample in the hands of a courier and sent him on a three-hour trip to a clinic whose computers were still working. Lorina and her mom waited in what became a largely empty ER, as most patients were sent away.

Ambulances racing to Essex Hospital were redirected elsewhere, as the Accident and Emergency department there had also stopped accepting patients. At North Hampshire Hospital, the CT and X-ray machines froze. Colchester Hospital canceled twenty-five operations. At Chesterfield Royal Hospital the problem was the reverse: without functioning computers, patients could not be released and had to spend another night in the hospital. It was May 12, 2017, and the British National Health Service had been hit by a ransomware cyberattack that was shutting down businesses all over Europe and North America, locking down computers and demanding payment in Bitcoin to unlock them.

The attack tool used became known as WannaCry, and seven months later the Australian, British, and American governments identified the culprit as one of the North Korean government's hacking groups, sometimes called the Lazarus Group by Western analysts. While WannaCry captured the media's attention in the United States and many other countries, the events in May were only a prelude to a much more devastating attack a month later by another state actor. Indeed, what was to come was the most devastating single cyberattack in history, so far costing companies more than $20 billion and, more importantly, shutting down key infrastructure.

While WannaCry got the public's attention, corporate and government IT security professionals had already been aware of the growing risk of ransomware. A year earlier, a virus known as Petya (named after a Soviet weapon in a James Bond movie) had demonstrated significant success in attacking Windows-based systems and then spreading encryption through- out the infected network. Analysis of Petya by U.S. cybersecurity firms later revealed that it employed an attack technique based on the National Security Agency's EternalBlue weapon.

Then in late June 2017, malware resembling Petya spread with unprecedented speed around the world, attacking Microsoft servers and then jumping to all connected devices on the affected corporate networks. In major companies seemingly selected at random, and at their facilities in scores of nations, computer screens froze and flashed messages demanding payment. It looked like ransomware again. It wasn't.

Once analysts realized it was not the Petya attack again, they creatively labeled the new attack NotPetya. What cybersecurity experts quickly surmised was that the demand for ransom was fake, a diversion. The attacking software was actually what was known as a wiper, which erased all software on the infected devices. Any device connected on an infected network would be wiped: desktops, laptops, data storage servers, routers, IP phones, mobile phones, tablets, printers.

Operations at major global corporations suddenly ground to a halt. At the pharmaceutical firm Merck, which made more than $40 billion in revenue in 2017 and employed more than sixty thousand workers, production lines froze. Distribution of vaccinations, oncology drugs, and hundreds of other pharmaceuticals stopped. Later, the company would claim the dam- ages cost them almost $900 million.

Maersk, a container ship and port giant, suddenly could not operate the cranes that move millions of shipping containers at its megaports around the world, including New York and New Jersey, Los Angeles,

and Rotterdam. Moreover, it had no idea where any given container was, what was in any container, or where any container was supposed to go. Later, the company would publicly own up to $300 million in damages, but a company insider told us that when opportunity costs were accounted for, the true loss was triple that number.

Hundreds of corporation, some in almost every sector, were frozen, including the logistics firm TNT Express (a subsidiary of FedEx), Mondelēz, the snack company, and the DLA Piper law firm. If there had been any doubt that a cyberattack could be global in an instant, that it could disable physical systems, or that it could affect the machinery that keeps the global economy movie, that doubt evaporated on June 27, 2017. Was it cyber war?

A Cyber War by Any Other Name

Whether NotPetya was an act of cyber war depends, of course, on your definition. Upon examination, NotPetya was an operation run by a military unit, specifically the Main Directorate of the General Staff of the Russian Federation's military, often called the GRU or Russian military intelligence. (In the funny-name-game world of cyber wonks, the GRU's hacking team is also known as Fancy Bear.)

The Russian military did not, we suspect, intend to indiscriminately attack global corporations. What it had intended was a crippling attack on Ukraine on the eve of its national holiday, Constitution Day. The GRU had figured out a truly creative attack vector, a channel that could be used to spread an attack.

What the GRU had noticed was that almost every company and government ministry in Ukraine used the same accounting software. Think of the prevalence of QuickBooks in the United States and you will get the picture. Only in Ukraine, the equivalent software was known as M.E.Doc, from the Ukrainian software company the Linkos Group. Like every other similar application, the M.E.Doc program was periodically updated. Updates were pushed out to licensed users from a server at Linkos. The updates were digitally signed by Linkos and recognized by users' firewalls, thus allowing the M.E.Doc updates to pass freely into corporate networks.

So the GRU hacked into Linkos and planted a little something extra in the next update to M.E.Doc: an attack package that exploited a known vulnerability in Microsoft server software, combined with a password-hacking tool and instructions to spread to any connected device on the network, wiping them of all software.

The GRU attack worked almost flawlessly, destroying about 10 percent of all devices in Ukraine, including some in every government ministry, more than twenty financial institutions, and at least four hospitals. *Almost* flawlessly. What the GRU had apparently not recognized (or maybe they did) was that global companies operating in Ukraine would also be hit, and from their Ukrainian offices the attack would spread over virtual private networks (VPNs) and rented corporate fiber connections back to corporate headquarters in England, Denmark, the United States, and elsewhere.

This kind of mistaken collateral damage is not unique to NotPetya or to the GRU. The software used in the so-called Stuxnet attack on the Iranian nuclear enrichment plant reportedly carried out by the United States in 2010 somehow got out into the world, even though the Natanz plant was not connected to the internet or any other network. Stuxnet quickly spread around the globe, was captured by cybersecurity teams in many countries, and was decompiled, with parts of it later reused in new attack tools.

Stuxnet, however, did not damage anything outside of Natanz, because it was written in a way that the only thing it could hurt was the Iranian nuclear enrichment processor. Nonetheless, the fact that the software spread way beyond its target was reportedly one of the motivations for President Obama's subsequent directive, Presidential Policy Directive 20, which allegedly restricted further offensive use of cyber tools without his personal approval. (President Trump is reported to have removed those restrictions in 2018.)

Stuxnet revealed to the world, or at least to anyone who cared enough to bother to grab a copy, one of the most sophisticated attack tools ever, containing more than fifty thousand lines of computer code including numerous tricks never used before (so-called zero-day exploits). NotPetya revealed not a thing about Russian GRU attack tools. It exposed nothing of theirs because it was not their tool. It was America's.

Using Our Weapons Against Us

An obscure, important, and contentious debate among cybersecurity experts concerns whether it's the responsibility of the U.S. government to tell software developers (say, Microsoft) when NSA hackers find a mistake in the company's code that would permit someone to do something new and malicious, such as hack in and copy customer data, steal money, or wipe out all the software on a network. In the parlance of U.S. government cyber-policy makers, this debate is called the "equities issue" because it involves balancing the interests of intelligence agencies trying to attack with the concerns of government departments such as Treasury and Homeland Security that have an interest in more secure corporate networks.

If the government tells the software developer, then the company issues a "patch" that can fix the problem. If the government does not tell them, then it can hack into interesting foreign networks using the vulnerability in order to learn things to protect the country. (The government creates an "exploit," a hacking tool that takes advantage of the poorly written computer code.)

After Edward Snowden stole sensitive NSA information and gave it to WikiLeaks (and the Russians), Obama appointed a five-man group to investigate and make recommendations. Dick Clarke was one of the group that became known as the Five Guys, after the Washington hamburger chain.

The Five Guys' recommendations were all made public, every single word of them, by the Obama White House. One of those recommendations was that when the NSA finds a hole in widely used software, it should tell the manufacturer, with rare exceptions. Those exceptions would be approved at a high level in the government and should be valid for only a finite period. The Obama administration accepted that recommendation.

Microsoft has charged that the NSA knew about a big problem with Microsoft's server software for five years and did not tell them. Instead, the NSA developed an attack tool, or zero-day exploit, and called it EternalBlue. Presumably, the NSA used EternalBlue to get into foreign networks. Only in March 2017 did Microsoft, having just been informed of its software's deficiencies by the U.S. government, issue a patch for the problem.

As is always the case when a software company issues a patch, not every one of its users gets the message or believes the warning that it is a critical patch that has to be installed right away. So, despite the patch, the North Korean authors of WannaCry were successful in using the vulnerability two months later,

in May 2017, and the Russian GRU used it again, in combination with other tricks, in creating the June 2017 NotPetya disaster.

Those devastating attacks would almost certainly have been avoided if the U.S. government had told Microsoft years earlier. At least, that is what Microsoft said publicly after it figured out what happened.

Why did the government finally tell Microsoft? Our guess, and it is just that, is that by March 2016 the government had figured out that Russia had stolen the U.S. attack kit, knew about the zero day, and was using it or was about to use it.

It is possible that the Russian GRU stole the zero-day attack tool from the United States in 2016, or perhaps even as early as 2013. We do know that another contractor assigned to the NSA, Harold Martin, was apparently walking out of NSA facilities with highly classified papers and software on a regular basis, according to the charges brought against him by the Justice Department after the FBI arrested him in 2016.

Martin used antivirus software to defend his personal home computer; specifically, he used Kaspersky Anti-Virus. Kaspersky, which is widely used around the world, is made in Russia. According to press reports, the Russian

GRU gained access to Kaspersky's Moscow headquarters and then used the millions of Kaspersky Anti-Virus packages installed on computers around the world to search for documents with certain keywords. (Kaspersky denies that this is what happened.)

Maybe the GRU learned those keywords, which may have been Top Secret Exceptionally Controlled Information code names, from the Edward Snowden treasure trove. In any event, one possibility is that, using a back- door in Kaspersky Anti-Virus on Harold Martin's home computer, the Russian GRU found a ton of NSA attack tools, perhaps including the EternalBlue exploit.

Now, how would anybody know that the Russian GRU did that? Well, it just could be that Israel's military intelligence Unit 8200 was sitting inside Kaspersky's network watching it all go down. The Israeli's would have told the NSA pretty quickly if that happened. It is also possible that the Russian GRU hacked a secret server, in the autumn of 2013. Maybe that was how they got the NSA's crown jewels.

However they got them, they got them. We know that because they posted them online for all the world to see, and use, in the summer of 2016. Posing as the fictional hacker group known as the Shadow Brokers, the Russian GRU started to dole out the NSA's attack tools publicly. It's true that they did not call them the NSA's tools, opting instead to call them property of the "Equation Group," but the NSA PowerPoint slides were kind of a giveaway as to who the Equation Group really was. The Shadow Brokers went on to offer to sell some of the Equation Group's better tricks. The tricks all seemed to date from 2013, which may give credence to the staging server attack as the source of the NSA's attack tools.

The NSA is not the only U.S. government organization engaged in cyberattacks. The Pentagon's Cyber Command is too, as is the CIA. We know a lot more about what the CIA does now because, like the NSA, it also had a major theft and public exposure of its cyber secrets. In the case of the CIA, however, there is little doubt about how the secrets were taken or by whom.

Joshua Schulte, a CIA employee, was arrested by the FBI in August 2017 and charged with passing over eight thousand pages of highly classified information to Julian Assange, who subsequently posted them publicly on the WikiLeaks website. Assange, an Australian who had taken refuge in Ecuador's London embassy, has been accused by numerous American authorities of acting in cooperation with Russian intelligence.

The CIA documents were called Vault 7 by WikiLeaks, and they too revealed numerous zero-day exploits of widely used software, including products of Apple, Microsoft, and Samsung (e.g., allegedly a tool to listen to rooms in which Samsung televisions were installed, even when the television appeared to be turned off). When the documents became public, Microsoft president Brad Smith had told them about the vulnerabilities.

At least one other U.S.-based company had, however, been noticing some of the alleged Vault 7 exploits. For at least six years, cybersecurity company Symantec had been reporting on attacks by a group it names Longhorn. Attack techniques used by Longhorn in more than sixteen countries reportedly match almost exactly in technical detail some of what was revealed in the Vault 7 documents. If that is true, then the CIA might have been exploiting flaws in U.S.-manufactured software for years without telling the companies involved.

WikiLeaks, which is not the most credible source of impartial information, alleged that the Vault 7 documents showed the existence of a CIA program code-named UMBRAGE. This program supposedly involved the CIA using attack tools that it had stolen from other governments in order to leave a misleading trail and cause investigators to believe attacks done by the CIA were, in fact, done by others.

By 2018, the outing of one another's cyber tools and personnel was picking up speed. An anonymous group calling itself Intrusion Truth began to regularly disclose the hacks, tools, and people involved in Chinese hacking groups known as APT 3 and APT 10. It is not yet generally agreed upon among the cyber-expert community who Intrusion Truth is, but it is clear that they are revealing the secret activity of the Chinese government.

What does all of this tell us? First, stealing one another's attack tools may be more widely practiced than was previously thought, and may be done by at least a few nations.

A second obvious observation from these incidents is that the security of U.S. cyberattack units is still miserably poor years after a frustrated Pres- ident issued an Executive Order (EO 13587) and other instructions to fix it. Most of the theft of U.S. attack tools could have been prevented by simple physical security procedures.

Third, we should not conclude that the Russian GRU has to steal U.S. attack tools. They have plenty of good ones they have developed themselves. Their motive in stealing and publicly releasing the U.S. cyber arsenal is to embarrass the United States, make it seem like America is the world's most problematic hacker, and allow nations (including our friends and allies) to go back and identify U.S. intelligence operations against them (thereby creating distrust among allies).

Finally, there is obviously a great deal of hostile activity by the militaries of various nations going on in cyberspace. All of this might not constitute war according to the traditional definition, but it is fairly clear by now that the United States and its allies have been regularly attacked by the Russian military using cyber weapons. The Russian military has not only used cyber weapons to collect intelligence, but has also deployed cyber weapons to damage, disrupt, and destroy physical objects in the real world, beyond the realm of 1's and 0's. And the Russians are not the only ones. To quote the British Foreign Office, the Russians are simply the most "reckless and indiscriminate"

Russia's GRU successfully penetrated the Pentagon's classified intranet, as well as the State Department and White House systems. According to the United Kingdom's National Cybersecurity Center in October 2018, the GRU has engaged in a sustained campaign of low-level cyber war for several years, going back at least to its 2007 attack on Estonia and its 2008 attack on the nation of Georgia.

According to the U.K., the GRU, operating under the false flag name of Sandworm, attacked the Ukrainian power grid in 2015 and again in 2016. Operating under the false flag name of Cyber Caliphate (sounds like an Arab terrorist group, right?), it shut down a French television network, TV5Monde. It attempted to interfere through cyberattacks in the investigations of the Russian assassination attempt in Bristol, England, Russian doping of Olympic athletes, and the Russian downing of Malaysia Airlines Flight 17.

Famously, the Russian GRU penetrated the Democratic National Committee (which admittedly required little skill) as one part of a multifaceted campaign to affect the outcome of the U.S. presidential election. And of course, there was the most damaging cyberattack in history to date, Not- Petya, about which the White House issued a rare public statement of attribution regarding a cyberattack.

In one operation in the Netherlands, GRU hackers were arrested in the parking lot of the international organization that investigates chemical weapons use, attempting to hack into the wi-fi. According to Dutch police, the Russian military personnel were in possession of taxi receipts from GRU headquarters to Moscow airport, thus proving that business expenses are the bane of every organization, even cyber-war units.

Whether or not you call all of that activity cyber war, it is objectively a lot of damage being done by a military organization. Much of it fits the definition we suggested in Cyber War in 2010 (damage, disruption, and destruction of physical objects caused by nation-state-created cyberattack). Back then there were commentators and critics who thought such predictions were hyperbolic. By now, however, it seems generally accepted that this kind of warfare can happen. Indeed, U.S. Director of National Intelligence Dan Coats publicly stated that the Russian government had penetrated the control systems of some U.S. electric power companies, that we were in a period similar to the months before 9/11, and that "the warning lights are blinking red."

The Russian GRU's teams such as Unit 26165 and Unit 74455 are not the only military organizations running around cyberspace breaking things. The Chinese People's Liberation Army (PLA) teams such as Unit 61398 and Unit 61486 have penetrated thousands of networks in the United States and tens of thousands around the world. Although President Obama and Pres- ident Xi signed an agreement to limit cyberattacks on each other for commercial purposes (about which more later), Chinese penetrations of U.S. organizations continue.

Similarly, North Korea's Bureau 121 and Unit 180 have helped to finance the development of missiles and nuclear weapons with their criminal theft activities around the world, including against the SWIFT international financial transfer system. North Korea has also attacked infrastructure and businesses in South Korea, including banks and television networks. The global attack that was WannaCry demonstrated the havoc that the North Koreans can wreak.

Iran's military, through its Revolutionary Guard Command (IRGC) and its Ministry of Intelligence, have also been damaging and disrupting in cyberspace. For weeks in 2012 the online banking systems of the eight largest U.S. banks were shit own by an Iranian attack, which the Justice Department later charged was directed by the IRGC. Iran penetrated the U.S. Navy Marine Corps Intranet and defied U.S. efforts to evict them for more than two years. Iranian units took control of networks running systems as diverse as a water system dam in New York State and the Sands Casino in Las Vegas.

Iran's destructive efforts also include the 2012 attack on the Saudi oil company Aramco, which wiped software off thousands of machines, and the 2017 penetration of the Triconex safety-instrumented

system of a petrochemical plant in Saudi Arabia, an attack apparently intended to prevent alarms going off during a planned lethal chemical leak in the future.

And then there is the United States, where in September 2018 the President devolved authority to conduct cyberattacks to the Department of Defense and instructed the military to "defend forward" to disrupt other nations' cyber activities. We will discuss that more in chapter 12.

Naming Cyber Warriors

One way in which the U.S. government has decided to respond to these cyber- attacks by foreign militaries has been to "name and shame." At the risk of compromising what are called sources and methods, U.S. intelligence agencies have permitted Justice Department lawyers to name, show photographs of, and issue arrest warrants for individuals in foreign military cyber units involved in attacks inside the United States. This U.S. tactic is intended to demonstrate the extent of the problem, to give the appearance of doing something about it, and in rare instances to make it possible to arrest and interrogate the military personnel involved. We found no U.S. government or former U.S. government official who thought it would deter further attacks.

Among those military personnel indicted in U.S. courts is Park Jin Hyok of the North Korean Reconnaissance General Bureau. From the People's Liberation Army, Huang Zhenyu was publicly accused and an arrest order was issued for him, among others. GRU officer Dmitriy Sergeyevich Badin is among a host of Russian military officials now sought by international law-enforcement agencies on a warrant from the United States. Ehsan Mohammadi is among the Iranians named by the U.S. Justice Department as having hacked American organizations on behalf of the Iranian government.

Though it has historically been challenging to apprehend foreign hackers because of their ability to conduct cyber operations from their own soil, some of the named military hackers have actually been arrested. Yanjun Xu of the PLA was arrested on a trip to Belgium. Alexei Morenets of the GRU was picked up by Dutch counterintelligence police in that parking lot in the Netherlands.

We have to leave it to your imagination how the United States knows the true names of these and many other foreign cyber military officers, how it obtained their pictures, and how it knows that they were involved in specific attacks. While you ponder that, keep in mind that the important thing here is that these are foreign military officers charged with attacking things in the United States.

Instability in Cyberspace Risks Escalation

All of this activity by Russia, China, North Korea, Iran, and, yes, the United States is suggestive of a dangerous pattern of crisis instability. Most significant hacking used to be done by non-state actors, individuals, or clubs. Now, major attacks are usually the work of some nation's military.

Nations are regularly using their militaries not only to steal secrets, but to damage, disrupt, and destroy sensitive systems inside potential enemy nations. Such operations could easily lead to escalation into broader war, intentionally or unintentionally. The U.S. military, for example, has said that it reserves the right to respond to cyberattacks with any weapon in its arsenal. To be clear, the recent and current levels, pace, and scope of disruptive activity in cyberspace by the military units of several nations is unprecedented,

dangerous, and unsustainable in "peacetime." It cannot continue like this. Either we control and deescalate tensions, or conditions will cease to have any resemblance to peacetime.

If we do not take concerted steps to reduce the risk of cyber war, if we do not engage in a multifaceted program to bring us closer to cyber peace, we risk highly destructive cyberattacks that could cripple modern societies and escalate into the kind of Great Power conflict we have not seen in more than seventy-five years. Thus, we need to make it a major national priority to find ways of defeating nation-state hackers. Some companies may already know how.

There are two lessons we could draw from the NotPetya attack on Ukraine. The first is that nation-state military and intelligence organizations are already taking down major global companies such as Maersk and Merck with cyberattacks. The second lesson, however, is the dog that did not bark. There were other U.S. and global companies in Ukraine during the NotPetya attack, companies such as Hyatt Hotels, Abbott Laboratories, Boeing, DowDupont, Eli Lilly, Johnson & Johnson, Cargill, Pfizer, Delta Air Lines, and John Deere. They do not appear to have been significantly damaged by NotPetya. We turn to what keeps some companies comparatively more secure in the next section.