CHAPTER XII

LEFT OF LAUNCH

MARY LOUISE KELLY (NPR): Is there a Stuxnet for North Korea?

JOHN BRENNAN (CIA DIRECTOR UNDER PRESIDENT OBAMA): [Laughter] Next question.

—December 2016

IN THE SPRING of 2016, North Korea's missiles started falling out of the sky—if they even made it that high.

In test after test, Kim Jong-un's Musudan missile—the pride of his fleet—was exploding on the launch pad, crashing seconds after launch, or traveling a hundred miles or so before plunging prematurely into the Sea of Japan. For a missile that Kim imagined would enable him to threaten the American air base on Guam and form the technological basis for a larger missile that could reach Hawaii or Los Angeles, the failures were a disaster.

All told, Kim Jong-un ordered eight Musudan tests between mid-April and mid-October 2016. Seven failed, some spectacularly, before he ordered a full suspension of the effort. An 88 percent failure rate was unheard-of, especially for a proven design. The Musudan was based on a compact but long-range missile the Soviets had built in the 1960s for launching from submarines. Its small size but high power made it perfect for Kim's new strategy: shipping missiles around the country on

mobile launchers and storing them in mountain tunnels, where American satellites would have trouble finding them.

As part of his effort to boost the range and lethality of the North's missile fleet, Kim had invested heavily in modifying the Soviet engines. The Musudan was far more complex than the Scud, the short-range missiles the North had made billions selling to Egypt, Pakistan, Syria, Libya, and Yemen, among other nations. Developing the Musudan technology was critical for Kim: He hoped it would pave the way for a whole new generation of single-stage and multistage missiles. With those in his arsenal, he could make good on his threat that no American base in the Pacific—and ultimately no American city—would be beyond his reach.

The North had been in the missile-launching business for a long time and had gained a reputation for mastering the art. So the serial run of Musudan failures in 2016—three in April, two in May and June, then two more in October, after the North had taken a pause to figure out what was happening to them—was confounding. The history of missile testing suggested that everyone suffered a lot of failures in the beginning, then figured it out and made things work. That's what happened during the race between the United States and the Soviet Union to build intercontinental ballistic missiles in the 1950s and '60s, an era marked by many spectacular crashes before the engineers and missileers figured out the technology. The Musudan experience reversed the usual trend. After years of successful tests of other missiles, it was as if North Korea's engineers forgot everything they'd learned.

Kim and his scientists were highly aware of what the United States and Israel had done to the Iranian nuclear program, and they had tried to insulate themselves from the same kind of attack. But the high failure rate of the missiles forced the North Korean leader to reassess the possibility that someone—maybe the Americans, maybe the South Koreans—was sabotaging his system. By October 2016, reports emerged that Kim Jong-un had ordered an investigation into whether the United States had somehow incapacitated the electronic guts of

the missiles, perhaps getting inside their electronics or their command-and-control systems. And there was always the possibility that an insider was involved, or even several.

After each North Korean failure, the Pentagon would announce that it had detected a test, and frequently would even celebrate the missile's failure. "It was a fiery, catastrophic attempt at a launch that was unsuccessful," a Pentagon spokesman told reporters in April 2016, after the first full test of the Musudan, timed to celebrate the birthday of the country's founder, Kim Il-sung. When subsequent attempts failed, the official news release from the Pentagon included dryly worded boilerplate that "The North American Aerospace Defense Command determined the missile launch from North Korea did not pose a threat to North America." The statements never speculated about what went wrong.

But there was a lot of speculation inside the Pentagon, the NSA, and the White House, among the select group who knew about the classified US program to escalate cyber and electronic attacks against North Korea, with a particular focus on its missile tests. Each explosion, each case of a missile going off course and falling into the sea, prompted the same urgent question: "Was this because of us?"

It had been more than two years since Obama, alarmed by North Korea's progress, had pressed the Pentagon in early 2014 to drastically accelerate the effort to bring down North Korea's missiles—and turned again to cyber and electronic sabotage for the solution to geopolitical tensions. A lot had happened since then. The Sony attack had focused the administration's attention on North Korea, but on its cyberattacks, not its missile program. The negotiations with Iran—which led to a deal in the summer of 2015 that shipped 97 percent of Iran's nuclear fuel out of the country, setting back its efforts by a decade or more—consumed the attention of Washington's nuclear experts. Russia emerged as a far greater aggressor, and China demonstrated, with surprising vigor, that it was in search of influence, economic dominance, and a military presence in places it had never before ventured. The emergence of Donald Trump made for captivating television as he transformed from a late-show punch line to an unstoppable candidate.

Through it all, Obama's North Korea sabotage effort churned ahead, silently.

The Obama administration's hope, of course, was that after two years of figuring out how to get inside North Korea's missile program, the United States had developed a worthy successor to Olympic Games: a way to delay by several years the day when the North would be able to threaten American cities with nuclear weapons. "It's too late to roll back the nuclear weapons program itself," William Perry, the former secretary of defense, told me. "Disrupting their tests would be a pretty effective way of stopping their ICBM program." It was the US government's only hope. The public strategy—which the White House briefly called "strategic patience"—was a failure. No diplomacy was under way. A military strike was far too risky. That left only covert action. And in countering proliferation, as one veteran of the process said to me wearily, "the best you can do is buy time."

The American-led cyber and electronic attacks on North Korea's missile program were vastly more complicated than the plan to go after the underground centrifuges in Iran years before. The Natanz nuclear plant was a comparatively easy target: It was a fixed site in a highly wired society, where engineers, diplomats, business executives, and scholars flowed in and out—all potential candidates to bring the malware into the country. And as the NSA and the Mossad were writing code to destroy the underground centrifuges, they had the luxury of time. As one veteran cyber warrior noted, if you got the code wrong, you could take it back to the shop, tinker with it, and try again in a week, a month, or six months. If the centrifuges then spun up or down too quickly and destroyed themselves, it was a pretty good bet the code had worked.

Going after North Korea's missiles was a completely different challenge. Access was miserable. The missiles were fired from multiple sites around the country, and increasingly from mobile launchers, in an

elaborate shell game that was intended to mask the time and location of launches. And timing was everything. There was a tiny window for action to interfere with a launch: just as the missile was being fueled and prepared for liftoff, or in the seconds just after liftoff.

Even as North Korea's missiles exploded or fell into the sea, it was maddeningly difficult to understand exactly why. What proportion, if any, of the North's troubles arose from Obama's initiative? And what proportion was from other causes? Indeed, throughout the Pentagon and at the NSA and Cyber Command, the project targeting North Korea's missile program had created a lot of skeptics who doubted that a cousin of Olympic Games explained the North's troubles.

With every Musudan launch, the raw data about how the missiles performed—speed, trajectory, engine performance—were picked up by American early warning satellites and radar. The information then flowed back to the Pacific Command in Hawaii, to the Strategic Command in Omaha, and to Adm. Rogers's teams at Cyber Command and the NSA. The data were then picked apart by the Korea hands and weapons-of-mass-destruction experts at the CIA and fed into the computers of the Defense Intelligence Agency's Missile and Space Intelligence Center in Huntsville, Alabama. "I bet NASA didn't spend as much time breaking down moon launches as we've spent looking at Kim's missile tests," one American official later told me.

But in the end, no one could convincingly determine whether the program Obama had ordered was working. When the missiles flew or shattered, they took with them the best evidence of their precise condition at the time of failure. Centrifuges slowed, but missiles vanished. The teams of cyber and electronic experts who had been targeting the North Korean systems for years would show up at the Pentagon and draw a direct line from the cyber and electronic warfare program to Kim Jong-un's rocket troubles. Clearly, they had a strong interest in making that case: They wanted to show results from the huge, secret American investment in cyberweapons, at least in part to secure funding for new initiatives at Cyber Command. But according to several

officials, they could never prove that any individual launch failed because of American interference.

Then the missile analysts would arrive, with alternative explanations. Yes, they conceded, the high rate of failure could have been accelerated because of the all-hands-on-deck effort to find ways into North Korea's systems. But there was no way to tell for sure. There were other possible explanations. The failures could have happened because of bad parts—especially because the United States and its allies had been running programs for more than a decade to get inside the North's supply chain. Or they could have happened because the North Korean engineers weren't as smart as they thought they were. Or maybe they were welding the rocket casings wrong.

"You have to be cautious whenever the enthusiasts of cyberattacks come in and claim victory," one former official advised me.

Whatever the true reason, the American plan to throw the missiles off-course succeeded at one thing: It made Kim Jong-un and his quartet of missile builders paranoid. The four members of the leadership who showed up in photographs surrounding the young leader during launches were clearly wondering whether sabotage, incompetence, or a series of unlucky accidents was the source of their misfortune. In that regard, the cyber sabotage effort initiated by the United States triggered the same kind of anxieties in North Korea that Stuxnet had caused in Iran, where the centrifuges seemed to be spinning normally—until unexplained disaster struck. The psychological effects may have been as important as the physical effects.

Nonetheless, the notoriously volatile young North Korean leader—known for executing his uncle and mounting a nerve-gas attack that killed his half-brother—proved remarkably tolerant when it came to the shortcomings of his rocket team. "We have never heard of him killing scientists," said Choi Hyun-kyoo, a researcher in South Korea who runs NK Tech, which manages a database of North Korean scientific publications. "He is someone who understands that trial and error are part of doing science."

Kim's missile whisperers could only hope his leniency would continue.

Before the North Korean missiles began blowing up, I remembered only vaguely hearing the term "left of launch."

I knew the basics: that "left of launch" meant working to stop missiles *before* they were fired, when they are presumably easier to target. The phrase had an echo from the war in Iraq, where the military often used the shorthand "left of boom" to describe their effort to find and dismantle roadside bombs before they did damage.

But as a matter of international law and geopolitics, "left of launch" was far more fraught. At its core was the idea that the United States was prepared to mount a strike against another nation in peacetime, getting inside their infrastructure to attack their missile and command-and-control systems before they could be used against the United States. Of course, if a president ordered such a strike in the traditional way—say, by sending bombers in to destroy a missile base in peacetime—it would likely trigger a war. The hope was that by turning to cyberweapons or other sabotage, the United States could slip in far more subtly, deny responsibility for whatever happened, and get away without being caught.

Not surprisingly, on the rare occasions when the Pentagon talked about "left of launch" in public—and it did not happen often—they made it sound far more benign. They never used the word "preemption," knowing that word would raise a host of legal and political problems, starting with the obvious one: that only Congress can declare wars. Officials never even described "left of launch" as one of the president's options for covert action, something he could initiate by signing a presidential "finding" authorizing the intelligence agencies to take action in the defense of the United States.

Instead, "left of launch" was treated simply as another form of missile defense, a way to improve the chances of success for more traditional missile defenses—the antimissile systems that were supposed to hit an incoming nuclear warhead before it reached American shores.

Those traditional systems needed all the help they could get. The United States began working on antimissile defenses after the Soviet Union test-fired the world's first ICBM in 1957. That launch spurred President Dwight D. Eisenhower to initiate a crash program that swept in many of the nation's best scientists. Sixty years and more than $300 billion later, the concept of traditional missile-defense systems hadn't changed much. The aim was still to "hit a bullet with a bullet"—in other words, to intercept a warhead in midflight with a precision-guided antimissile system launched, often into space, from Alaska, California, or a ship at sea.

Given the number of Soviet missiles that could be launched at once, any American system would be overwhelmed. Later, after the Soviet Union fell, President George W. Bush focused on North Korea, which at the time could only hope to lob a few missiles in the direction of the United States. In late 2002, Bush announced that his administration was deploying long-range antimissile interceptors at a giant, muddy base just south of Fairbanks with a sister installation in California.

Once again, optimism outran experience. The number of successful interceptions in trial runs was embarrassing—roughly 50 percent, and that rate of success was achieved in tests conducted under ideal conditions. Soon the Pentagon stopped making public any quantifiable measurements. The truth was just too painful. Whenever senators pushed for more details, someone would tell them they would be happy to take it up in a classified session.

In light of these disappointments, at the Pentagon, and even among the defense contractors who were dependent on multibillion-dollar contracts for traditional missile interceptors, "left of launch" grew in importance. If missiles could be stopped on the ground, or in the first few seconds of flight, the interceptors would not have to be launched at all—they would become a backup defense, instead of a primary defense. The savviest of the contractors, eager to bid on the new business, began talking about "missile defeat" programs instead of "missile defense" programs. But the biggest of those contractors quietly worried

that if cyber and electronic methods of taking down missiles proved too successful, they could put their multibillion-dollar traditional antimissile programs out of business. The big money was still in bending metal and making interceptors—not in writing code.

"This stuff is a double-edged sword," one person advising a major defense contractor told me. "Everyone wants it to work. But they don't want it to work too well."

WASHINGTON HID MANY of the details of the effort in plain sight.

When Bill Broad and I began asking around the Pentagon and the White House in 2016 about the surprising number of North Korean missile failures, we were not surprised to be met with stony silences. After the Stuxnet leak investigation, no one wanted to be accused of talking about a cyber-sabotage program—especially one that might not be working. But there were occasional hints that the answers lay in the "left of launch" program.

Bill dug into the open literature. Soon he showed up with a grin at my desk in Washington toting an inch-and-a-half-thick pile of Pentagon testimony and public documents. For a secret program, he noted, people sure had said a lot, mostly because they were lobbying for money.

The trail started with Gen. Martin E. Dempsey, chairman of the Joint Chiefs of Staff when Obama was pushing for the stepped-up attacks. Shortly after the North Koreans set off a nuclear test in February 2013, Dempsey publicly announced a new "left of launch" effort that would focus on "cyberwarfare, directed energy, and electronic attack." It was part of a larger presentation at the Pentagon on technologies that needed to be in place over the next seven years, and almost no one noticed the "left of launch" piece. But the plain fact was that the nation's top military officer had explained that malware, lasers, and signal jamming were all becoming important new adjuncts to the traditional methods of halting potential enemy strikes.

General Dempsey never mentioned North Korea in his statement. He didn't have to. A map accompanying the policy paper the Pentagon issued on the subject showed a missile from North Korea streaking toward the United States. That freed others to use similar imagery.

Soon Raytheon, the largest missile-defense contractor, started talking openly at conferences about the new opportunities in "left of launch" technologies, particularly cyber and electronic strikes executed at the moment of launch. A Raytheon document from one of its industry conferences, which was posted on a public website until we began asking questions about it, was not exactly subtle. One slide showed a range of adversaries against whom "left of launch" was particularly well suited, with a picture of a solemn Kim Jong-un sandwiched between Vladimir Putin and Xi Jinping. A chart illustrating how the program worked featured a bright band separating the steps that Raytheon's technology could accomplish to defeat missiles before and after launch. The most interesting part was the band itself—representing the minutes right around launch. There, Raytheon had inserted the words "cyber" and "EW," or electronic warfare, indicating that was the time to strike the launch process, at its most vulnerable point.

The chart showed that the cyber and electronic strikes could also target enemy factories—the latest effort at using industrial sabotage to slow the North. The program required a huge and complex effort, involving America's national laboratories, the Energy Department, and the CIA, and it was deployed against Iran as well. But it was hardly a surefire approach. The North Koreans were learning how to build more and more of their systems indigenously, and were even beginning to make some of the highly volatile rocket fuel that would power their longest-range missiles.

That progress made it all the more urgent that the National Security Agency and its Tailored Access Operations unit get inside the North's systems. Naturally, those operations remain among the most classified. But a tiny glimpse of the effort came from Oren J. Falkowitz, a quirky former NSA operator who started an innovative Silicon

Valley cybersecurity firm named Area 1. In a *Times* interview about his start-up, with my colleague Nicole Perlroth, he described how some of the company's approaches to anticipating cyberattacks were inspired by work done inside the NSA to break into computer systems for the North's missile program, in what he characterized as an effort to understand their missile-launch schedules.

Falkowitz said nothing about what the United States did with the information it acquired, which left open the question of whether we were just conducting espionage about launch schedules or were actively seeding implants in the North Korean systems. But there were other indications—some public, some whispered—of American successes in getting into the command-and-control systems. It was hard gaining access to the North's sealed-off computer networks, former American and South Korean operators reported. But once inside, they said, the North's digital defenses fell pretty quickly. North Korea's military, one noted, was as paranoid as Iran's, but not as talented.

A review of a gathering of top antimissile experts at the Center for Strategic and International Studies in 2015 gave us even more details. Archer Macy Jr., a retired navy rear admiral, described how the Pentagon was developing ways not only of preventing successful missile launches but also of interfering in their flight paths and navigation systems. That was followed by congressional testimony in which James Syring, the director of the Pentagon's Missile Defense Agency, described "left of launch" strikes as "game changing" because they reduced the need to "rely exclusively on expensive interceptors."

Every once in a while during these conferences and hearings, someone would touch on the profound question at the core of the program. That happened one day when Kenneth Todorov, a retired air force brigadier general, asked how the United States would justify what amounts to preemptive war under international law: attacking the North's missile launches first, before any strike, to gain a strategic advantage. "Are we, as a military and a nation," he asked, prepared to "go after potential targets in advance?" And if so, are we ready for other nations to do the same to us?

Todorov was getting at a critical point that has been periodically debated since President Bush, in 2002, declared that preemption was back as a central American principle for dealing with a hostile world. If the United States saw a missile on a North Korean launch pad being fueled, loaded with a warhead, and seemingly intended for American territory or that of an ally, it would likely be within its rights under international law to take out the missile on the pad.

But "left of launch" suggested a different scenario: A *preventive* strike, the kind that one state executes against another in the absence of an imminent threat. Think Pearl Harbor, or of a strong state that strikes a weaker but rising competitor while it still can. That is largely forbidden by international law.

With cyberstrikes—invisible, deniable—the temptation to conduct preventive war may be higher than it has ever been before. Unsurprisingly, few government officials want to delve too deeply, at least in public, into how the laws of war apply to offensive cyber action.

In private they debate these issues constantly. But as Robert Litt, the former general counsel to the director of national intelligence during the Obama years, put it to me one day: "There is no issue on which government lawyers have spent more time, to less productive effect, than on the question of how the laws of war apply to cyber."

In March 2016, just as North Korea was stepping up testing of its prized Musudan missile, I tried to engage Donald Trump on the subject of what he thought about America's new cyber arsenal—and how he might use it if elected. Trump was at Mar-a-Lago, his Florida golf club, and my colleague Maggie Haberman and I were interviewing him as part of a detailed conversation he'd agreed to with the *Times* on the subject of national-security issues.

My goal in trying to get him to talk about cyberweapons in that interview was simple: I wanted to see whether a candidate who spoke about military power as if it were still 1959—tanks and aircraft carriers and nukes—had given any thought to new technologies. For anyone

new to the world of diplomacy, coercion, and military planning, the first step would be to understand the newest tools in the toolbox.

Digital warfare was new stuff for him; as the conversation went on, it wasn't clear he had ever heard of the American cyber operations against Iran. His main interest was to demonstrate, on cyber and all other issues, that he would be tougher and more decisive than Barack Obama, even if he wasn't quite certain what Obama had done in the cyber arena. He made an argument that, as with so many other things in Trump's worldview, America was blowing its lead:

> We're the ones that sort of were very much involved with the creation, but we're so obsolete, we just seem to be toyed with by so many different countries, already. And we don't know who's doing what. We don't know who's got the power, who's got that capability, some people say it's China, some people say it's Russia. But certainly cyber has to be a, you know, certainly cyber has to be in our thought process, very strongly in our thought process. Inconceivable that, inconceivable the power of cyber. But as you say, you can take out, you can take out, you can make countries nonfunctioning with a strong use of cyber. I don't think we're there. I don't think we're as advanced as other countries are, and I think you probably would agree with that. I don't think we're advanced, I think we're going backwards in so many different ways. I think we're going backwards with our military . . . we move forward with cyber, but other countries are moving forward at a much more rapid pace.

It was more assertion than analysis, more declaration than doctrine. We were trying to get Trump to discuss when it is justifiable to use cyber-weapons; he took the conversation to the question of who is stronger and who is weaker, unencumbered by many facts.

Then, just to reinforce his campaign talking points, he concluded with: "We are frankly not being led very well in terms of the protection of this country."

Ten months later, Trump was inaugurated as the forty-fifth president and inherited a complex cyber operation against a hostile state that he barely understood. In the meantime, Bill Broad and I had built a pretty compelling case that North Korea was the target of an intensive, sophisticated US effort to send its missiles awry. With more reporting, we arrived at some solid conclusions about how the attacks worked.

Then came the sensitive part: telling the government what we were preparing to publish, seeking their comments, and hearing them out if they believed any of our revelations could compromise an ongoing operation or put lives at risk. In the last weeks of the Obama administration, we met with intelligence officials, fully anticipating that their first reaction would be to tell us to refrain from printing a story on the sensitive subject. When they said nothing of the sort, we left the session thinking we still had more reporting to do.

That reporting ran into the chaos of Trump's inauguration and his tumultuous first month in office—the blitz of executive orders, Trump's growing paranoia about the Russia investigation, and his suspicion of a "deep state" out to undermine him and his agenda. We were not ready to publish until late February. That's when I called K. T. McFarland, then Trump's deputy national security adviser, and explained to her that I needed to come by and make sure the new administration was aware of a story about a major program they were inheriting.

The next day I showed up at McFarland's tiny West Wing office. Her boss, Lt. Gen. Michael Flynn, had just been fired days before for misleading Vice President Michael Pence about his conversations with the Russian ambassador to the United States, Sergey Kislyak. Flynn had denied talking to Kislyak about overturning election-related sanctions against Russia that Obama had imposed in the last weeks of his presidency; in fact, the topic had indeed come up during their conversations.

As I walked past the national security adviser's corner office, the door was open; someone had rolled up the carpet, stripped all the books off the shelves, and stacked Flynn's office chair on top of his desk. It

looked like a dorm room on move-out day, and certainly not the sight one expected to see a little more than a month into a new administration. It was a symbol of far more chaos to come.

While I knew the Obama transition teams had left binders full of briefing materials on North Korea for the new administration, I suspected few people had the clearances—or the time—to go through them all. Flynn, the former director of the Defense Intelligence Agency, was probably the one most current on the North Korean threat. But not only had he just been fired, his handpicked aides—derisively called "The Flynnstones"—were gradually being eased out.

When I sat down with McFarland, who had been a junior aide to Henry Kissinger in the White House forty years before, she told me that the administration had taken seriously Barack Obama's warning that North Korea would be their most immediate national-security problem. McFarland's job—in which she didn't last very long—was to convene the "deputies committee"—made up of the second- and third-ranking officials in State, Defense, Energy, Treasury, and the intelligence agencies—to tee up strategies for the president and his cabinet. Unsurprisingly, most of the initial meetings were about North Korea.

But as I began to describe to McFarland what we had learned about the "left of launch" program, and how it was being used against North Korea, I could see by the look on her face that it seemed to be the first she had heard of it. That was surprising: If there was anything that the new national-security team needed to get up to speed on quickly, it was the full range of American efforts to defang the North Korean threat. Perhaps she was just a good poker player, but the discussion did not suggest the new administration had a full grasp of what it was about to face.

After a half hour, McFarland said she had to go brief the president on a different matter. But she told me she saw no national-security issues in what we were planning to publish.

"It sounds like it will all work out," she said as she headed to the Oval Office.

She proved prematurely optimistic. After the word spread inside the administration, which had no experience dealing with sensitive national-security stories, the *Times* got a stiffly worded letter from the White House counsel, Donald McGahn, previously an election lawyer, accusing us of preparing to violate American national security—and hinting that the government might try to take some kind of action.

Within a few days Flynn's replacement as national security adviser, H. R. McMaster, invited us into his office to hear for himself what we were preparing to publish. It was his first full day on the job. A strategist with a PhD in military history, and the author of an incisive history of how the American military lied to itself about the war in Vietnam, his mind went straight to historical analogy.

"Is this the Enigma codes?" he asked, a reference to the encrypted German communications that the British cracked—a secret kept for decades. Broad and I told him we didn't think so: there was solid evidence that Kim Jong-un already understood the issue, and he had already shut down the Musudan tests after the string of failures.

McMaster had not had to deal with Korea or with cyber issues in-depth before; he made his name in the Persian Gulf and had been promoted through the ranks by Gen. David Petraeus. His most recent jobs had been running the Army Capabilities Integration Center, where he was tasked with thinking about future conflicts. But he was clearly still catching up on the scope of the Korea crisis.

He asked us to meet yet again with intelligence officials and talk through the details. A day later we descended into the Situation Room to review our findings with them. Based on previous discussions, we had already decided to omit technical details, including several that might give the North indications of where their systems were vulnerable. That was normal practice. But explaining what the United States was doing, we thought, was vital: As our executive editor, Dean Baquet, noted, there was no way for Americans to have an informed public discussion about the US response to the North Korea crisis without understanding our past struggles to deal with it. "This was one of America's most

urgent threats," he said, and that meant covering the American use of cyberweapons "the way we covered the Pentagon Papers, WikiLeaks, drone strikes, counterterrorism, and nuclear arms."

With publication imminent, McMaster went to brief Trump on what we were revealing—and what we were withholding. Trump had already ramped up his critique of the *Times,* and McMaster cautioned me that Trump might well take to Twitter to denounce the paper—hardly a first. In fact, on the morning that the story was published, Trump started a Twitter attack. But it wasn't about us.

"How low has President Obama gone to tapp [*sic*] my phones during the very sacred election process," he wrote that morning. "This is Nixon/Watergate." It was an accusation based on no facts.

Trump's tweet crystallized how his obsessions, and the chaos of the transition in the first six weeks of the new presidency, had prevented the new administration from focusing on what Obama had warned was the central national-security threat the nation faced. They had been left hundreds of pages of briefing materials about North Korea, but it appears little of it was absorbed. The questions swirling around the success or failure of the primary covert program to thwart the missile launches had not been fully engaged by McFarland, who was ousted in a few weeks, and they were entirely new to McMaster, who lasted just a bit more than a year.

Clearly Trump's mind was not yet on the dictator he would soon call "Rocket Man," or the country he would threaten to incinerate with "fire and fury." But positions were beginning to harden. Nineteen days before Trump's inauguration, Kim Jong-un had taunted the president-elect with a declaration that he was then in "the final stage in preparations" for an inaugural test of his intercontinental ballistic missiles—missiles larger and more sophisticated than the Musudan. Trump had responded, with typical Twitter bravado, "It won't happen."

It seemed inevitable that Trump would soon face the same challenge his predecessors did: how to deal with North Korea without prompting a broader war. He would confront issues that had been long

debated in the Situation Room: whether to order the escalation of the Pentagon's cyber- and electronic-warfare effort, crack down again on trade with crushing economic sanctions, open negotiations with the North to freeze its nuclear and missile programs, or prepare for direct missile strikes on its nuclear and missile sites.

It seemed clear to me that, still lacking a strategy, Trump's answer would likely be to attempt all four.

WHILE THE UNITED STATES struggled to sabotage Kim's missile program, the North's hackers were looking for new targets in the West. In the two years after the Sony attack, their cyber corps had learned a lot and grown more global. As a top cybersecurity official for one of the behemoths of Silicon Valley put it to me, "If there was a 'most improved' award for states looking to weaponize the Internet, the North Koreans would win it. Hands down."

While Americans were thinking about how to use cyberweapons to neutralize the North's missiles, the North was thinking about how to use them to pay for those missiles—a huge challenge for a country under every form of economic sanction. Which is how the North's hacking teams cooked up a plan to steal $1 billion from the Bangladesh Central Bank in 2016.

With their exquisite nose for vulnerable institutions, the North's hackers focused on Bangladesh in January, figuring their cyber protections had to be pretty minimal. It was a good bet. With just a few weeks of quiet digital observation of the bank, the hackers got all they needed: the procedures for transferring funds internationally, some stolen credentials, and an understanding of when the bank would be closed for a holiday that extended into a weekend. The extra days provided them with time to execute transfers before anyone was around to stop them.

The hackers put together transfer orders for just under $1 billion, including one transfer to the Shalika Foundation in Sri Lanka. That

proved the fatal mistake: In instructions to the New York Federal Reserve, through which such transactions flow, someone spelled "foundation" as "fandation." The error raised eyebrows, and the transfers were suspended—but only after Kim Jong-un's hackers had gotten away with $81 million. If it had been a physical bank heist, it would have been considered one of the largest and most brilliant in modern times. (By comparison, the great Brinks heist of 1950, in Boston's North End, swept up only about $2.7 million, worth about ten times that in modern currency.)

After the Sony hacks, the North had good reason to believe that any retaliation for their cyber exploits would be minimal, and they were right. There was no penalty for the Bangladesh bank attack, or cryptocurrency heists that followed.

"Cyber is a tailor-made instrument of power for them," Chris Inglis, a former deputy director of the National Security Agency, told me. "There's a low cost of entry, it's largely asymmetrical, there's some degree of anonymity and stealth in its use. It can hold large swaths of nation-state infrastructure and private-sector infrastructure at risk. It's a source of income."

At an earlier time, North Korea counterfeited crude $100 bills to finance the country's operations. That grew more difficult as the United States made the currency harder and harder to copy. But ransomware, digital bank heists, and hacks of South Korea's fledgling Bitcoin exchanges all made up for the loss of the counterfeiting business. Today the North may be the first state to use cybercrime to finance its state operations.

Bangladesh was hardly the only victim, and not even the first. In 2015 there was an intrusion into the Philippines, then the Tien Phong Bank in Vietnam. In February 2016 hackers got inside the website of Poland's financial regulator and infected visitors—from the central banks of Venezuela, Estonia, Chile, Brazil, and Mexico—in hopes of also breaking into those banks.

Then came two of the boldest attacks—one on South Korea, the other on the world.

There was no military document that the North wanted to read more than the American blueprints for war on the Korean Peninsula. Sometime in the fall of 2016, when most of the world was distracted by the presidential election, the North breached South Korea's Defense Integrated Data Center, according to Rhee Cheol-hee, a member of the South Korean parliament's National Defense Committee, and swept up 182 gigabytes of data—including OpPlan 5015, a detailed outline of what the US military delicately called a "decapitation strike." Rarely have the details leaked. But the documents the North's hackers stole appear to include strategies for finding and killing the country's top civilian and military leaders, and then wiping out as much of the mobile missile fleet and seizing as many nuclear weapons as possible. OpPlan 5015 would not stop there—the strategy included ways to counter the North's elite commandos, who would almost certainly slip into the South.

There is some speculation that the North intended to get caught stealing the war plan, in order to unnerve their adversaries and force them to rewrite it from scratch. We'll likely never know. But the theft is just one more sign of how deeply the North has compromised South Korea's sensitive networks. There is also evidence that Pyongyang has planted "digital sleeper cells" in critical infrastructure in the South in case they are needed to paralyze power supplies or command-and-control systems.

Then came WannaCry.

It is unclear how long the North Korean hacking team spent planning what the United States later charged was an "indiscriminate" attack on hundreds of thousands of computers, many in hospitals and schools. But it is clear how the hackers got inside: with some vulnerabilities in Microsoft software stolen from the NSA by the Shadow Brokers group. It was the ultimate cascading crime: the NSA lost its weapons; the North Koreans shot them back.

In this case, the hacking tool stolen from the NSA went by the name "Eternal Blue." It was a standard piece of the TAO's toolbox because it exploited a vulnerability in Microsoft Windows servers—an

operating system so widely used that it allowed the malware to spread across millions of computer networks. No one had seen anything like it in nearly a decade, since a computer worm called "Conficker" went wild.

In this case, the North Korean hackers married the NSA's tool to a new form of ransomware, which locks computers and makes their data inaccessible—unless the user pays for an electronic key. The attack was spread via a basic phishing email, similar to the one used by Russian hackers in the attacks on the Democratic National Committee and other targets in 2016. It contained an encrypted, compressed file that evaded most virus-detection software. And once it burst alive inside a computer or network, users received a demand for $300 to unlock their data. It is unclear how many paid, but those who did never got the key—if there ever was one—to unlock their documents and databases.

The hackers guessed correctly that while Microsoft had patched this hole in the system—after the NSA had warned the company about the vulnerability just two months before the attack—few people who used old Microsoft Windows systems would have gone to the trouble of updating their software. And when the attackers struck in the late afternoon of May 12, 2016, anybody with ancient computers and ancient software to match—like the National Health Service in the United Kingdom—was a sitting duck.

"Many of the computers that were the most adversely affected were running Windows XP," Brad Smith, the president of Microsoft, explained to me later. "It's an operating system that we released in 2001. And when you stop and think about it, you realize that was six years before the first iPhone. It was six months before the first iPod." Smith didn't use the other obvious historic marker: the operating system was released to manufacturers just eighteen days before the September 11 attacks, a moment that changed our national sensibility about our vulnerabilities.

WannaCry, like the Russian attacks on the Ukraine power grid in the previous two years, was among a new generation of attacks that put

civilians in the crosshairs. In that regard, it is akin to terrorism. "If you are wondering why you're getting hacked—or attempted-hacked—with greater frequency," said Jared Cohen, the former State Department official who now runs Alphabet's Jigsaw, a part of the Google parent company, which has done pioneering work in how to make people safer on the Internet, "it is because you are getting hit with the digital equivalent of shrapnel in an escalating state-against-state war, way out there in cyberspace."

Cohen is right: WannaCry is a prime example of where the newest cyber battles are headed. In the first years of state-on-state cyberwars, the targets of crippling hacks were mostly strategic, and often state-owned. Olympic Games was aimed at an isolated, underground nuclear enrichment facility. The attacks on ISIS were directed at vicious terrorist groups. The North Korea missile hacks were aimed at a program that directly threatened America and its allies.

But with WannaCry, the targeting seemed far more random, and the results were unpredictable. With computer systems of several major British hospital systems shut down, ambulances were diverted and nonemergency surgeries delayed. Banks and transportation systems across dozens of countries were affected. But it is doubtful the North Koreans knew, or cared, which systems would be crippled.

"I suspect the attackers had no idea what would be hit," one American investigator told me. "It was about creating chaos" and fear. Evidence of the untargeted nature of the malware lies in the fact that it hit seventy-four countries; after Britain, the hardest hit was Russia. (In what some might see as a sign of cosmic digital justice, Russia's Interior Ministry was among the most prominent victims.) Then Ukraine. Then Taiwan. There was no discernible political pattern.

Moreover, there was no warning. Britain's National Cyber Security Centre saw nothing coming, its director of operations, Paul Chichester, told my *Times* colleagues. In fact, investigators in Britain suspect the WannaCry attack may have been an early misfire of a weapon that was still under development—or a test of tactics and vulnerabilities.

"This was part of an evolving effort to find ways to disable key

industries," said Brian Lord, a former deputy director for intelligence and cyber operations at Britain's GCHQ. "All I have to do is create a moderately disabling attack on a key part of the social infrastructure, and then watch the media sensationalize it and panic the public."

For all the billions spent on cyber defenses, in the end the Cyber Security Centre, British intelligence, and Microsoft had little to do with bringing the attack to an end. For that they had to thank Marcus Hutchins, a college dropout and self-taught hacker who was living with his parents in the southwest of England. He spotted a web address somewhere in the software and, largely on a lark, paid $10.69 to register it as a domain name as the attack was under way. The activation of the domain name turned out to act as a kill switch; it kept the malware from continuing to spread. (Hutchins was later arrested in Las Vegas and charged with being the author of another kind of malware, one designed to steal banking credentials.)

It took months—until December 2017, three years to the day after Obama accused North Korea of the Sony attacks—for the United States and Britain to formally declare that Kim Jong-un's government was responsible for WannaCry. Thomas Bossert, President Trump's homeland security adviser, said he was "comfortable" asserting that the hackers were "directed by the government of North Korea," but said that conclusion came from looking at "not only the operational infrastructure, but also the tradecraft and the routine and the behaviors that we've seen demonstrated in past attacks. And so you have to apply some gumshoe work here, not just some code analysis."

Bossert was honest about the fact that having identified the North Koreans, he couldn't do much else to them. "President Trump has used just about every lever you can use, short of starving the people of North Korea to death, to change their behavior," Bossert acknowledged. "And so we don't have a lot of room left here."

The gumshoe work stopped short, of course, of reporting about how Shadow Brokers allowed the North Koreans to get their hands on tools developed for the American cyber arsenal. Describing how the NSA enabled North Korean hackers was either too sensitive, too

embarrassing, or both. And it was one of the most troubling parts of the whole incident.

While the US government says that it reports to industry more than 90 percent of the software flaws it discovers, so that they can be fixed, "Eternal Blue" was clearly part of the 10 percent it held on to in order to bolster American firepower. Microsoft never heard about the vulnerability until after the weapon based on it was stolen. Yet the US government acted as if it bore no responsibility for the devastating cyberattack. When I asked Bossert, and his deputy, Rob Joyce, who ran the TAO and clearly knew something of what happened to these pilfered weapons, they argued that the fault was entirely with those who used the weapons—not with those who lost control of them. It was a mystifying argument: if someone fails to lock up their guns, and a weapon stolen from their house is used in a school shooting, the gun owner has at least some moral or legal liability.

"It's a problem," Leon Panetta, the former defense secretary and CIA director told me one day as we discussed the WannaCry attacks, "when the US government can't hold on to its arsenal. We can't be in that position. And we wouldn't tolerate that explanation from other countries."

Brad Smith of Microsoft, clearly angry, compared the NSA's loss of its weapons to the air force's losing a Tomahawk Missile that was then shot back at an American ally. He pointed to the arrest of "an NSA contractor who had these weapons in his garage. And you don't see Tomahawk weapons in people's garages."

In fact, these days you did.

It was just two months later that Ukraine was hit with the NotPetya attack, which roused Dymtro Shymkiv to action from upstate New York. It was very similar to WannaCry, although NotPetya was the work of the Russians, the Trump administration said in early 2017. Those hackers had clearly learned from the North Koreans. They made sure that no patch of Microsoft software would slow the spread of their code, and no "kill switch" could be activated.

In short, they designed a more

thousand targets around the world, in more than sixty-five countries. Maersk, the Danish shipping company, was among the worst hit: they reported losing $300 million in revenues and had to replace four thousand servers and thousands of computers. NotPetya made the Sony strike, only three years earlier, look like the work of amateurs.

WHATEVER THE CAUSE of Kim Jong-un's missile troubles in 2016—sabotage or incompetence or bad parts or faulty assembly—he solved the problem in 2017.

At a speed that caught American intelligence officials off guard—to say nothing of the newly arrived Trump administration—Kim rolled out an entirely new missile technology. Clearly he had a parallel program running alongside the Musudan, and it was based on another decades-old Soviet engine design that powered intercontinental ballistic missiles.

Unlike the Musudan, this one worked, and it worked right away. In quick succession Kim demonstrated ranges that could reach Guam, then the West Coast, then Chicago and Washington, DC. Out of nine intermediate and long-range launch tests in 2017, only one failed. That was an 88 percent success rate—a startling improvement from the year before.

And on the first Sunday in September, Kim detonated a sixth nuclear bomb, one that was far more powerful than any the North had set off before. It was fifteen times greater in power than the atomic bomb that leveled Hiroshima. Kim had entered the big leagues of nuclear power.

Many have seen this coming. For twenty years public CIA estimates declared that North Korea would have this capability sometime before 2020, but Kim's burst of progress after such a string of failures the previous year had not been predicted. Like the Russia hacks during the US election, Kim's strategic move caught the intelligence world unawares.

I went back to see General McMaster in December 2017. He readily

acknowledged that Kim's race to the finish line—a bid to establish the North as a nuclear power before any negotiations began or sanctions took a more punishing toll—"has been quicker and the timeline is a lot more compressed than most people believed."

The question he and other officials would not touch, of course, was whether the North's string of successes in 2017 indicated that they had figured out the vulnerabilities of the Musudan—and solved them. What happened to "left of launch"? Were the new missiles less vulnerable to cyber and electronic attacks? Or had the supply chain changed, making it harder to infiltrate bad parts into the missile program? Or had the United States concluded it was simply being too obvious in attacking the Musudan and now was holding back until it was ready to strike at a larger missile?

There were plenty of indications that the US reliance on cyber tools was alive and well, just somewhat better hidden. Trump asked Congress in November 2017 for $4 billion in emergency funds for boosting missile defense and taking other steps to contain the North. Hundreds of millions of dollars were dedicated to what the budget documents called "disruption/defeat" efforts. Those efforts, several officials confirmed, include a more sophisticated attempt at cyber and electronic strikes. And there were several billion dollars allotted for traditional missile defense—even amid the doubts that it will work.

Trump's former CIA director, Mike Pompeo, occasionally hinted at ongoing programs, suggesting that the United States was "working diligently" to slow Kim's progress and delay the day when he was ready to put a nuclear warhead atop one of those missiles. Pompeo suggested that day was just "months away," but he repeated this estimate from early in Trump's administration through its first eighteen months. Jim Mattis, the defense secretary, had a darker take: after the North's most successful missile test, in November 2017, he said the country already had the ability to hit "everywhere in the world, basically."

AFTERWORD

SEN. DAN SULLIVAN (R-ALASKA): What do you think our adversaries think right now? If you do a cyberattack on America, what's going to happen to them?

LT. GEN. PAUL NAKASONE (COMMANDER OF US ARMY CYBER COMMAND): So basically, I would say right now they do not think that much will happen to them.

SULLIVAN: They don't fear us.

NAKASONE: They don't fear us.

SULLIVAN: So is that good?

NAKASONE: It is not good, Senator.

—Lt. Gen. Paul Nakasone's confirmation hearing, as commander of US Cyber Command, March 1, 2018

UNTIL THE CYBER age came along, America's two oceans symbolized our enduring national myth of invulnerability. The threat of nuclear attack preoccupied us during the Cold War, but generally

the United States has assured it could take out dictators, conduct drone strikes on terrorists, and blow up missile bases in faraway lands with relatively little fear of retaliation. There were exceptions, of course, moments of national terror: the British burned Washington in the War of 1812, the Japanese attacked Pearl Harbor, and al Qaeda brought down the Twin Towers and struck the Pentagon. But we knew the only attack that could threaten the existence of the country would come at the tip of a Soviet or Chinese intercontinental missile, or in the form of terrorists with access to nuclear weapons. And after some terrifying close calls, notably the Cuban Missile Crisis in 1962, we found an uneasy balance of power with our primary adversaries—mutually assured destruction—to deter the worst. It worked, or has so far, because the cost of failure is so high.

In the cyber age, we have not found that balance, and probably never will. Cyberweapons are entirely different from nuclear arms, and their effects have so far remained relatively modest. But to assume that will continue to be true is to assume we understand the destructive power of the technology we have unleashed and that we can manage it. History suggests that is a risky bet.

I keep on my desk a wonderful volume, *Airships in Peace and War*, first published in London in 1908 by military historian R. P. Hearne, which tried to imagine how a strange new invention of that time—airplanes—would change the course of history for Europe's great powers. One chapter is entitled "Could England Be Raided?" The question was answered in 1916, when the Germans first delivered scattered air attacks across the country. Within a year the first battles for control of the skies were under way. In 1940, the Blitz devastated London.

In the cyber world, we have not yet seen the equivalent of the Blitz. The early damage has been limited—centrifuges in Iran, a steel plant in Germany, a casino in Las Vegas, a crippled petrochemical plant in Saudi Arabia, missiles gone mysteriously awry in North Korea. Yet every week seems to bring hints of things to come, as city services became paralyzed by ransomware in Atlanta and patients were turned away after a cyberattack struck the health-care system in Britain.

The sheer acceleration in the number of attacks, and their rapidly changing goals, is one of several warning signs that we all are living through a revolution, playing out at digital speed.

IN THE EARLY days of this revolution, reaching for a cyberweapon seemed almost risk-free. Now that calculus is changing.

No one could blame an American president for using a remote-control weapon to crash Iran's nuclear centrifuges or disable North Korea's missiles. Given the choice between risking the lives of American soldiers or intelligence officers and reaching deep inside a country without setting foot in its territory, the decision seemed self-evident. The same logic that made drones so appealing to George W. Bush and Barack Obama—great stealth and low risk—made cyberweapons irresistible too. And in both Iran and North Korea, cyberweapons provided a way to slow dangerous military programs without triggering a war.

The harder question over the next decade will be whether reaching for such weapons with increasing frequency will continue to be a wise choice. By going into the North's missile systems, the United States set a precedent, just as we did with Olympic Games, that other nations will surely follow. While we talk publicly about setting norms for what should be off-limits for offensive cyber activity—hospitals, emergency responders, and now election systems—we are seen around the world as hypocrites. Every time the United States reaches into another nation's critical infrastructure, we make our own fair game for retaliation.

Yet we clearly are not prepared for the day when each American action in cyberspace triggers an escalating response. Because for now, as the stories told in the preceding pages make clear, deterrence is not working in the cyber realm. True, there has not been a devastating attack on the power grid, a "cyber Pearl Harbor" that might tempt an American president to make good on the threat contained in the 2018 Nuclear Posture Review, which is that some kinds of non-nuclear

attacks—chiefly, cyberattacks—may force the president to reach for the ultimate weapon.

The very fact that we need to make the threat underscores the failures of the past few years. When Adm. Michael Rogers took over the National Security Agency, he told me in his office in 2014 that his tenure would be measured by his success at convincing America's adversaries that there was a cost—a high cost—to attacking the nation's networks. "Right now, if you look at most nation-states—groups and individuals and the activity they are engaging in in cyber, very broadly, most of them seem to have come to the conclusion that there is little risk of having to pay a price for this in real terms," he said at Stanford later that year.

When his successor, General Nakasone, conceded in his confirmation hearing four years later that "they don't fear us," he was admitting that after spending billions of dollars on new defenses and new offensive weapons, the United States has still failed to create a deterrent against cyberattacks.

Perhaps that is understandable. In the Cold War, nuclear deterrence did not emerge instantly. It took years of collaboration between technologists, strategists, generals, and politicians. It involved a very public debate, which the United States seems unwilling to conduct in the cyber realm—for fear of revealing our capabilities, or having to surrender some of them.

In the nuclear era, deterrence worked well between the United States and the Soviet Union not only because each knew the other possessed world-destroying power, but also because each had confidence in the integrity of its own weapons system. Each was certain that if the president ordered a launch, the launch would happen.

But over the past few years we have seen time and again that cyberweapons can undermine that confidence. The Iranians lost all assurance they could control their centrifuges. The North Koreans suspected someone was messing with their launch systems. And inside the Pentagon there is growing fear that one day in the not-too-distant future an American commander could order a launch and missiles would not fire.

We experienced a less deadly version of that loss of confidence in 2016, when we feared that Russian hackers were seeking to break into our election systems, looking for ways to alter voter-registration data. Even if they failed, the mere attempt was enough to undercut public confidence in the outcome of the vote. Imagine a similarly skilled group breaking into America's nuclear early-warning systems, triggering a fake warning that the United States was under attack. It could prompt a president to launch our own weapons before the chimerical incoming missiles could strike.

This may sound like the stuff of a bad thriller, but almost exactly that scenario—without the cyber manipulation—nearly triggered disaster in 1979, when a watch officer awoke William Perry, then an undersecretary of defense, to report that an early-warning system was showing two hundred incoming ICBMs. The military quickly determined it to be a false alarm: someone had placed a training tape, simulating an incoming attack, into the real warning system. However, Perry later warned, if an enemy attempted the same thing with a sophisticated bit of malware, perhaps placed by an insider, "we might not be so lucky next time."

The implications of having our own command-and-control system compromised underscore why sabotaging similar systems in other nations is dangerous business. If American leaders—or Russian leaders—feared their missiles might not lift off when someone hit the button, or that they were programmed to go off-course, it could easily undermine the system of deterrence that has helped reduce the likelihood of nuclear war for the past several decades. It could also encourage countries to build more missiles—as an insurance policy—and perhaps to launch them earlier.

"It's not hard to imagine how we greatly increase the risk of stumbling into a conflict because of an accident, or inadvertence, or just deliberate deception," James Miller, a former undersecretary of defense for policy, and one of the country's most experienced nuclear strategists, told me after he and Richard Fontaine finished a study of just that problem. "It's conceivable that other states, and even non-state

actors, could undertake cyberattacks that lead to an inadvertent escalation with Russia," Miller concluded. That a president could make snap decisions on which millions of lives depend, based on information that had been subtly manipulated, is sheer madness.

General Nakasone's warning that countries do not fear us—one he uttered just weeks before becoming the new director of the NSA and commander of United States Cyber Command—focused on the question of whether the United States can retaliate after its networks are struck. But there are other ways to deter attacks—chiefly by convincing your adversaries that your defenses are strong, and they will not succeed. In the lingo of strategists, this is called "deterrence by denial." If an attack would be futile, why bother in the first place?

Deterrence by denial requires an exquisite defense. And while American intelligence officials will not concede the point, internal government assessments say it will be a decade—at least—before the United States can reasonably defend our most critical infrastructure from a devastating cyberattack launched by Russia or China, the two most skilled adversaries in the field. There are simply too many vital networks, growing too quickly, to mount a convincing defense. Offense is still wildly outpacing defense. As Bruce Schneier, a cyber expert whose work is a must-read on the topic, put it so well: "We are getting better. But we are getting worse faster."

Schneier's point is that even as we build far greater defenses, our vulnerabilities are expanding dramatically. With huge investments, the top tier of the financial industry and the electric utilities have done the best job of safeguarding their networks—meaning that a North Korean hacker aiming at those industries would likely have more luck targeting smaller banks and rural power companies. But as we put autonomous cars on the road, connect Alexas to our lights and our thermostats, put ill-protected Internet-connected video cameras on our houses, and conduct our financial lives over our cell phones, our vulnerabilities expand exponentially.

During the Cold War, we learned how to live, uneasily, with the knowledge that the Soviet Union and China had nuclear weapons

pointed at us. There were no perfect defenses. In a world of constant cyber conflict we will have to adjust similarly.

Yet if we are more vulnerable than ever, why is the Pentagon talking about the need to conduct a far more aggressive cyber strategy? In testimony to Congress in early 2018, the leaders of the NSA and Cyber Command pressed the case that if the United States is to prevail in the new era of cyber conflict, our forces need to be unshackled. Even if we see attacks massing, they said, the current rules of engagement keep us from attacking the attackers. It is time, they argued, to start "hacking the hackers."

The approach Cyber Command described and detailed in its strategy documents is one of nearly daily raids behind enemy lines, looking for threats before they reach America's own computer networks. "The United States must increase resiliency, defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage," one of those documents said—all military-speak for taking the war to the enemy.

It was an instinct born of more than a decade of counterterrorism operations, where the United States learned that the best way to take on al Qaeda or ISIS was by destroying them at their bases and in their living rooms. But in cyber it amounts to an admission that our defenses at home are wildly insufficient and that the only way to win is to respond to every perceived threat. As with many of Trump's new strategies, taken to its logical extreme this approach carries enormous risks of miscalculation and escalation. To pull it off, the United States would have to scrap the requirement that the president authorize every destructive cyberattack. Cyber operations would begin to look more like evening raids conducted by Special Operations Forces. The problem is that when other countries adopt the same strategy, as inevitably they will, the chances rise dramatically that cyberattacks will accelerate and could trigger a shooting war, or worse.

. . .

So WHAT IS to be done?

The first step is to recognize the folly of going on offense unless we have a good defense. We would be lucky to seal up three-quarters of the glaring vulnerabilities in American networks today. But the best way to deter attack—and counterattack—is deterrence by denial. That requires a major national effort, far beyond the civil defense projects of the 1950s when the United States built a highway system that could evacuate civilians and dug shelters in large cities. A parallel effort to secure America's cyber infrastructure has often been discussed, but it has never happened. It is complicated by the fact that the main targets of attack are in private hands. Given the complexity of the Internet, the government can't regulate how banks, telecom firms, gas pipeline companies, and Google and Facebook design their cybersecurity. Every one of those systems is radically different.

For that reason, even after a decade of debate it's still not clear who in the federal government, if anyone, is responsible for defending the country—and the economy—from the most sophisticated cyberattacks. Homeland Security is supposed to "coordinate," but just as we expect the Pentagon to defend the United States against incoming missile attacks, there's a presumption that it will defend American companies and individuals against sophisticated, state-sponsored hacks (but not against scammers, teenage hackers, and trolls living in Saint Petersburg). It's time to get real. The government isn't going to play a role in protecting American institutions except when it comes to the most critical of infrastructures: the electric grid, the voting system, the water and wastewater systems, the financial system, and nuclear weapons. Once we've understood this fact, we need a Manhattan Project to lock down our most critical systems. That will take presidential leadership.

Even then, civil defense will not be close to enough. One of the lessons of the past few years is that the dynamic of cyberattacks is completely different from what we grew accustomed to during the superpower standoffs of the twentieth century. We have to adjust our strategy to reflect that we will be far more vulnerable than almost any other major nation for years to come. As Michael Sulmeyer, a former Pentagon official now running a Harvard cyber initiative, has observed, "When it comes to cyberspace . . . the United States has more to lose than its adversaries because it has gone further in embracing innovation and connectivity without security. But although the societies and infrastructure of Washington's adversaries are less connected and vulnerable, their methods of hacking can still be disrupted. . . .

"If the United States hopes to win," he continued, "it should spend less time trying to persuade its competitors that it is not worth hacking and more time preempting them and degrading their ability to do so. It is time to target capabilities not calculations."

What does that mean in the real world? Obviously, the United States is not going to respond to every cyberattack; we would be in constant low-level war. Not every cyberattack needs a cyber response. Criminal attacks should be handled as other crimes are handled—with rigorous prosecution. The United States is getting better and better at that: the indictments of Iranian and Chinese hackers—even if they are still at large—and the extradition of a major Russian cyber criminal in 2018 show there are ways of responding short of treating every hack as if it is an attack.

And as in everything else in global affairs, red lines matter. So when trolls from the Internet Research Agency began bombarding the United States with fake news from fake accounts—with the intent of meddling in an American election—they needed to be delisted from Facebook. (That happened, but not until well after the election.) If the agency remained undeterred, its servers needed to be melted down, courtesy of our cyberweapons. The servers would be replaced, of course, perhaps quickly. But the message would be sent, and the Russians would know that the United States was able and willing to respond.

And while the intelligence agencies would insist on secrecy, that would defeat the point: for our response to deter attackers, it needs to be very public—as public as an American airstrike on a chemical-weapons

plant in Syria, or an Israeli strike on a nuclear reactor. Every time we respond quietly—or not at all—to an attack because we are worried about revealing the quality of our detection systems or the capability of our weapons, we only encourage escalation and further cyber strikes from our adversaries.

For the same reason, the United States needs to open up about some of our own offensive cyber operations, especially if their details have been revealed. To this day the United States has not admitted its role in Olympic Games. It was, after all, a covert operation—and covert operations are not to be discussed, by law. But what if, once the code was traveling around the world and it became widely known that Stuxnet was an American-Israeli creation, both Washington and Jerusalem had publicly owned up to their role? What if they had admitted to it, the way Israel acknowledges, implicitly or explicitly, that it has bombed reactors in Iraq and Syria? We might well have established one of those red lines: if you produce nuclear fuel in violation of UN mandates, expect that something bad could happen to your centrifuges—maybe from the air, maybe from cyberspace.

Most important, just as the United States must show other nations there is a price to pay for truly serious cyberattacks, we must also show that some things are off-limits. And until America discusses publicly—at the presidential level—what we *will not* do in cyberspace, we have no hope of getting other countries to limit themselves as well.

It will be easier to navigate those decisions when the government acknowledges a few realities.

The first is that our cyber capabilities are no longer unique. Russia and China have nearly matched America's cyber skills; Iran and North Korea will likely do so soon, if they haven't already. We have to adjust to that reality. Those countries will no sooner abandon their cyber arsenals than they will abandon their nuclear arsenals or ambitions. The clock cannot be turned back. So it is time for arms control.

Second, we need a playbook for responding to attacks, and we need

to demonstrate a willingness to use it. It is one thing to convene a "Cyber Action Group," as Obama did fairly often, and have them debate when there is enough evidence and enough concern to recommend to the president a "proportional response." It is another thing to respond quickly and effectively when such an attack occurs.

Third, we must develop our abilities to attribute attacks and make calling out any adversary the standard response to cyber aggression. The Trump administration, in its first eighteen months, began doing just this: it named North Korea as the culprit in WannaCry and Russia as the creator of NotPetya. It needs to do that more often, and faster.

Fourth, we need to rethink the wisdom of reflexive secrecy around our cyber capabilities. Certainly, some secrecy about how our cyberweapons work is necessary—though by now, after Snowden and Shadow Brokers, there is not much mystery left. America's adversaries have a pretty complete picture of how the United States breaks into the darkest corners of cyberspace.

But the intelligence agency's insistence on secrecy—the refusal to discuss offensive cyberweapons in any detail—makes it impossible to debate how precisely these weapons can be targeted and whether some should be banned because of their potential threat to civilians. We cannot expect Russian and Iranian hackers to stop implanting malware in our utility grid unless we are willing to talk about giving up our own implants in their power grids. We cannot insist that the US government has the right to a "backdoor" into Apple's iPhones and encrypted apps unless we are willing to make the Internet less safe for everyone, because any backdoor will become the target of hackers around the globe.

No country likes giving up military or intelligence capabilities. But we have done it before. America swore off chemical and biological weapons when we determined that the cost to civilians of legitimizing them was greater than any military advantage they offered. We limited the kinds of nuclear weapons we would build, and banned some. We can do the same in cyberspace, but only if we are willing to openly discuss our capabilities and to help monitor cyberspace for violators.

Fifth, the world needs to move ahead with setting these norms of behavior even if governments are not yet ready. Classic arms-control treaties won't work: they take years to negotiate and more to ratify. With the blistering pace of technological change in cyber, they would be outdated before they ever went into effect. The best hope is to reach a consensus on principles that begins with minimizing the danger to ordinary civilians, the fundamental political goal of most rules of warfare. There are several ways to accomplish that goal, all of them with significant drawbacks. But the most intriguing, to my mind, has emerged under the rubric of a "Digital Geneva Convention," in which companies—not countries—take the lead in the short term. But countries must then step up their games too.

Microsoft's president, Brad Smith, is one of the strongest advocates of the concept. He imagines loosely modeling a cyber accord among companies on traditional warfare conventions that have evolved for more than a century. Over the decades the rules have broadened and deepened, embracing the treatment of prisoners, the banning of chemical weapons, the protection of noncombatants, and the kind of aid that should be provided to the wounded, no matter whose side they fought on.

The analogy to cyberspace is hardly exact. The Geneva Conventions apply in wartime; if there is hope for an analogous set of rules of the road in cyber, they will need to set standards for peacetime. And they must apply to companies as well as countries, since Google, Microsoft, Facebook, and Cisco form the battlespace in which the world's cyber conflicts are fought.

In the spring of 2018, about three dozen companies—Microsoft, Facebook, and Intel among them—agreed to the most basic set of principles, including an innocent-sounding vow that the signatories would refuse to help any government, including the United States, mount cyberattacks against "innocent civilians and enterprises from anywhere." The companies also committed to come to the aid of any nation on the receiving end of such attacks, whether the motive for the attack is "criminal or geopolitical."

It was a start, but a barely satisfying one. No Chinese, Russian, or Iranian companies were part of the initial compact, nor were some of the biggest forces in the technology world, including Google and Amazon, both still struggling between their desires to do vast business with the US military and their desires to avoid alienating their customers. The wording of the accord left lots of maneuvering room for the companies to join attacks against terror groups, or even against governments repressing their own citizens. Moreover, the principles made no mention of supporting democracy, or human rights—meaning that Apple, if it later joined the accord, could still get away with its decision to bow to Beijing by keeping its data on Chinese customers on servers inside China. In other words, the first principles were like the Internet—sprawling and messy.

"I have no illusions this will be easy," Smith told me in Germany at the beginning of 2018. "We're going to need laws passed that make clear that certain principles need to be respected around the world, that governments need to refrain from attacking critical infrastructure in times of peace or war, or even when it's unclear whether we're at a time of peace or war." Of course, the Geneva Conventions have been regularly violated, in world wars and civil wars, from Vietnam to Syria.

There's no such thing as fully protecting civilians. Individual citizens don't have the option of going on the offense, and most have no interest in becoming combatants in a global cyber conflict. But over time, these principles have made the world more humane.

Still, there are steps individuals should take to protect themselves and help to avoid becoming collateral damage. Awareness—about what phishing campaigns look like, about how to lock up home-network wi-fi routers, and about how to sign up for two-factor authentication—can help to wipe out 80 percent or so of the daily threat. If we wouldn't leave our doors unlocked when we leave home, or the keys in the ignition of our cars, we shouldn't leave our lives exposed on our phones, either.

None of that will stop a determined, state-sponsored adversary. Houses can be protected against everyday burglars, but not against incoming ICBMs.

The lesson of the past decade is that, unless shooting breaks out, it will always be unclear if we are at peace or war. Governments that cannot stand up to far larger powers with conventional armies will have little incentive to give up the advantages that cyberweapons offer. We are living in a gray zone, one of constant digital conflict. That is not a pleasant prospect, but it is the world we have created for ourselves. To survive it, we must make some fundamental decisions, akin to ones we made after the invention of the airplane and the atomic bomb—decisions that enabled us to navigate a constant state of peril.

Now, as then, we have to think more broadly about where our security will be found. Clearly, it is not in an unending cyber arms race where victories over adversaries are fleeting, and where the greatest objective is to break another nation's encryption or turn off its factories. We need to remember that we built these technologies to enrich our societies and our lives, and not to find yet another way to plunge our adversaries into darkness. The good news is that because we created the technology, we have a chance of controlling it—if we concentrate on how to manage the risks. It has worked in other realms. It can work in cyberspace as well.

ACKNOWLEDGMENTS

The Perfect Weapon grew out of my reporting for *The New York Times*, but it is also a follow-on to a world I began to explore in *Confront and Conceal* (Crown, 2012). That book was the first to tell the story of Olympic Games, the American-Israeli cyber effort aimed at Iran's nuclear program. At the time it was published, it was hard to find more than a handful of examples of cases in which states used cyberweapons against each other. Scarcely six years later, that is a daily occurrence. So, not surprisingly, the ambitions for a book that explained this era grew, and with it so did my indebtedness to editors, researchers, and colleagues.

Let me start at the *Times*, where I have worked for nearly thirty-six years, in Washington and overseas. Arthur Sulzberger Jr. and A. G. Sulzberger, our previous and current publishers, have been unstintingly generous in letting me roam the world to explain to our readers this new and frightening age. And they never complained about the legal bills. Dean Baquet, our executive editor, and Joe Kahn, the managing editor, have championed these stories, and pressed for more. So have Matt Purdy, Susan Chira, and Rebecca Corbett, who offered ideas, fine editing, and encouragement along the way.