CHAPTER 1

ORIGINAL SINS

This has a whiff of August 1945. Somebody just used a new weapon, and this weapon will not be put back in the box.

—Gen. Michael Hayden, former director, National Security Agency and Central Intelligence Agency

On an early spring day in 2012, I drove along the winding, wooded driveway of the Central Intelligence Agency and pulled up in front of what the agency quaintly calls its "Old Headquarters."

I knew that the meeting I was headed to—with Michael Morell, the agency's deputy director—was likely to be difficult. A few weeks before, the White House had asked me to see Morell and talk with him about an especially sensitive story the *Times* was preparing to publish. The two of us had met briefly in the West Wing basement office of Benjamin J. Rhodes, then the deputy national security advisor for strategic communications, as I explained what I had learned: how two presidents of strikingly different temperaments, George W. Bush and Barack Obama, had both come to the decision to use the most sophisticated cyberweapon in history against Iran as the last, best chance to forestall a new war in the Middle East.

Neither Rhodes nor Morell seemed surprised that I had pieced the story together; the weapon's code, called "Stuxnet," had accidentally spread around the world nearly two years before, making it evident

that someone was using malware in an attempt to blow up Iran's nuclear facilities. Stuxnet was filled with digital fingerprints and other clues about where and when it had been written. That someone eventually would follow those clues to discover the plan that had launched it seemed inevitable. The operation, which I learned through months of reporting had been code-named "Olympic Games," was simply too big, and involved too many players, to stay secret forever. The Iranians themselves had long ago declared, with relatively little proof, that the United States and Israel were behind the attack. But neither government had ever uttered an admission, emblematic of the reflexive secrecy they wrapped around all cyber operations.

As is true with nuclear weapons, only the president could authorize the American use of a cyberweapon for destructive purposes. Yet because virtually all offensive cyber operations take place as covert actions, which by law must be designed to be deniable, no American president had ever been caught authorizing one. The *Times* piece would lay out the Situation Room debate over using a cyberweapon to mount the kind of attack that, previously, could have been executed only by bombing or sending in saboteurs.

But as I walked across the famous atrium of the CIA—its walls dotted with bronze-colored stars, one for each of the CIA officers who had died in defense of the country—and headed up the elevator to Morell's office, there was no way for me to know how the story threatened to disrupt the web of secrecy the United States had built around its decade-long race to build up its cyber capabilities. Nor could I have known that I would touch off one of the larger federal leak investigations of modern times, or that it would lead to the unfair prosecution of a military officer who was highly valued by Obama and who was among the cohort who had brought the US military into the era of modern cyberwarfare.

It turned out that the US government was not yet ready to discuss the consequences of its decision to use cyberweapons against an[illegible] in peacetime. Nor was it eager to assess the degree to which

America's actions contributed to a cyber arms race that Iran, Russia, North Korea, and China had joined.

BEYOND THE OFT-PHOTOGRAPHED lobby, the CIA's well-worn executive offices resembled those of the declining computer firms—like the now-extinct Burroughs and Digital Equipment Corporation—that I had covered decades ago as a young technology reporter. The retro look prevailed especially on the seventh floor, in the suite that Allen Dulles, CIA director under Eisenhower and Kennedy, designed so that he could sit within feet of his deputy director as they oversaw the vast and complex Cold War effort to steal secrets and take down adversaries. Appropriately, the look of the world's most famous spy agency was a bit deceiving: As the story of Olympic Games made clear, the agency was deeply into the digital age. But it had no interest in overtly displaying its prowess.

I had come to the Old Headquarters to hear about which details of the emerging story so concerned Morell and his colleagues that they were preparing to ask the *Times* to withhold them, lest we tip off other targets of ongoing operations. By their nature such conversations are fraught. News organizations must be willing to listen to government concerns, but insist, for obvious First Amendment reasons, that the decision to publish belongs to them, not the government. Morell, while always friendly and professional, had already indicated that, in his view, none of the Olympic Games story should be published. But he was a realist, and knew that the accidental revelation and dissemination of the Stuxnet worm meant the story was not going to disappear. For the CIA, that day's meeting was an exercise in learning what I had learned, and in directing damage control.

Operation Olympic Games was largely the work of the NSA and Israel's Unit 8200, its military cyber operation. But the CIA, I had learned over time, played a key part, executing a presidential authorization for covert action—known in Washington as a "finding"—to

slow Iran's nuclear program. Because "findings" are secret and intended to be denied publicly, I had no expectation that the agency officials I saw that day would acknowledge their role in deploying the weapon, much less the subsequent destruction of roughly one thousand centrifuges that had been spinning beneath the Iranian desert. And they did not.

But something about this story was different, and it added to the tension over its forthcoming publication. Cyberweapons, among the first strategic weapons created by the intelligence agencies rather than by the military, had been swaddled in more secrecy than that surrounding nuclear and biological weapons, or new generations of stealth fighters and drones. There was an assumption inside the government that anything published about the use of cyberweapons would impede their future use. While the government would describe in great detail its outrage about cyberattacks against the United States—or even trace evidence that other powers had entered the networks of our banks or electric systems—it considered the most basic conversations about US capabilities, intentions, or doctrines off-limits. Even some inside the US government deemed this level of secrecy ridiculous: How could you begin to discuss setting international rules about the use of weapons you won't acknowledge owning, much less using?

Clearly, there was no consensus within the Obama administration about how these weapons should be used. Even while Obama was approving new strikes on the Iranian nuclear plant, he harbored his own doubts. As our story explained, in meetings in the Situation Room in the first year of his presidency, Obama had repeatedly questioned whether the United States was setting a precedent—using a cyberweapon to cripple a nuclear facility—that the country would one day regret. This was, he and others noted, exactly the kind of precision-guided weapon that other nations would someday learn to turn on us. "It was the right question," said one senior official who came into the administration after the Stuxnet attacks were over. "But no one understood how quickly that day would come."

Curiously, Obama had already proven willing to engage in a public argument over similar questions about drones. Everything about drone warfare had been secret when he came to office, but over time Obama made elements of the program public and proved willing to explain the law and reasoning behind his decision to deploy these remote-controlled killing machines. In doing so, he gradually lifted the secrecy surrounding the use of drones so that the world could understand whether they were hitting terrorists, and when they went awry and killed children or wedding guests.

Cyberweapons were different. The government would barely admit to owning them, much less talk about the rules for when and why it used them. But the issues were very similar; just as investigative reporting about the unintended costs of drone strikes had forced the debate about unmanned weapons, my editors and I felt a journalistic imperative to explain to readers how the government was embracing cyberweapons that could ultimately be turned against our homeland. Olympic Games had opened the door to a new dimension of warfare that no one fully understood.

The only thing that was clear was that there would be no backpedaling. When Michael Hayden, who had been central to the early days of America's experimentation with cyberweapons, said that the Stuxnet code had "the whiff of August 1945" about it—a reference to the dropping of the atomic bomb on Hiroshima and Nagasaki—he was making clear that a new era had dawned. Hayden's security clearances meant he couldn't acknowledge American involvement in Stuxnet, but he left no doubt about the magnitude of its importance.

"I do know this," Hayden concluded. "If we go out and do something, most of the rest of the world now feels that this is a new standard, and it's something that they now feel legitimated to do as well."

That is exactly what happened.

. . .

Hayden was well practiced at talking about Stuxnet as if he were an outsider looking in, a zoologist who had just observed the odd behavior of an animal and declared the discovery of a new species. But in fact, he likely knew exactly what he was looking at. Hayden served as director of the CIA during the early days of Olympic Games. By that time, he was already in the vanguard of those who, in the mid-1990s, came to believe that cyberweapons were not simply a new tool but also what war fighters call a "new domain": the place where future power conflicts great and small would play out.

As Hayden rose through the ranks of the air force in the 1970s, everyone agreed on the four physical domains that had long defined warfare: People had fought on land and sea for millennia, and in the air since World War I. Space was added in the 1950s and '60s, when satellites begat antisatellites, and intercontinental ballistic missiles led to antiballistic missile systems. But cyberspace? As one long-retired general once asked me with genuine mystification at the Air Force Academy in Colorado Springs, "How do you fight in a place you can't see?"

Hayden's insight into the game-changing nature of cyber conflict began to form more than twenty years earlier, when he was assigned to San Antonio, Texas, as the commander of the Air Intelligence Agency, an air force unit that gave him an early glimpse of the power of a new generation of electronic weapons. He remembered watching in wonder as members of the staff disabled remote workstations and used electronic-warfare techniques to fool a radarscope that was trying to track a fighter plane. But what struck him most, fresh back from the wars in the Balkans, was how relentlessly the US military was coming under regular attack in peacetime.

The year after Hayden got to Texas, in 1998, the FBI was called in to investigate seemingly bizarre intrusions that had begun popping up in strange places connected to military or intelligence networks, from the Los Alamos and Sandia National Laboratories—where nuclear weapons are designed—to universities, such as the Colorado School of Mines, which held a significant contract with the Navy. There

was a particular concentration of intrusions around the networks of Wright-Patterson Air Force Base in Ohio, located on the site where the Wright brothers once tested many of their early planes.

It was a computer operator at the School of Mines who first discovered the hack, after he saw some nighttime computer activity he could not explain. The attack turned out to be a very large one, and persistent, seemingly coming from Russia. The hackers had lurked in some of these systems for two years and had stolen thousands of pages of unclassified material concerning sensitive technologies.

Shock soon gave way to the accompanying recognition of a new reality. The attack was given the name "Moonlight Maze." The Russians were initially helpful in the investigation, until they realized that the FBI had evidence that it was the Russian government, not some teenage hackers, behind the intrusions. Moscow shut down its cooperation. John Hamre, the bookish, usually unflappable defense scholar who was serving as deputy secretary of defense, told Congressional intelligence committees, "We're in the middle of a cyberwar."

"This was a real wake-up call for us," Hamre told me. "Until then, we'd had incursions, but never a case of a foreign power that broke into our systems and simply wouldn't leave—and was hard to evict."

Some experts who have studied the intrusion argue that Moonlight Maze never really ended; it just morphed into new attacks that continued for the next two decades. Whatever the truth, the Russian attacks galvanized the first serious efforts by the United States to defend its networks and form its own offensive cyber forces.

The attack forced the United States to confront the implications of the digital age. As Hayden noted, in the 1980s, when he was based in Korea, a military communication would be typed, scanned, sent to Washington, and then printed for someone to deal with as if it were just another piece of classified paper. But suddenly emails and classified cables became the default mode of communication and gave skilled intelligence agencies worldwide a way to intercept a far wider range of information "in transit."

The explosion of digital data gave the NSA a new mission. The agency responsible for encrypting and protecting sensitive information, mostly for the military and intelligence agencies, zeroed in on a vast new set of targets: computer data stored around the world that was vulnerable to the NSA's fast-growing cadres of hackers. Much of this information was not the kind of "data in transit" the NSA had spent decades intercepting. Instead, it was locked away in computer complexes that foreign governments, in their naïveté, had viewed as largely invulnerable. That was a fantasy, of course. An agency that had spent decades intercepting electrons flying through phone lines and over satellites was suddenly focused on what they called "data at rest." And getting that data meant breaking into computer networks around the world.

"This was all about going to the end point, the targeted network," Hayden later wrote, rather than waiting in hopes a message could be plucked out of the sky. And that required figuring out how to break into systems. Soon the NSA, CIA, and Pentagon joined forces to create an organization, blandly called the Information Operations Technology Center, designed to do just that.

The center was regarded with enormous suspicion by old-timers at the CIA who thought it represented game playing by people who should be doing real spying. But these veterans were living in a lost world. In retrospect, by the early 2000s the United States was entering a new arms race, akin to the one in which it had invested billions for the first hydrogen bomb, then the first intercontinental ballistic missiles, and later still missiles with multiple warheads. But even the Pentagon didn't know how to think about these new weapons or where to put them in its vast bureaucracy. Donald Rumsfeld, returning in 2001 to the post of secretary of defense, which he had held in the late 1970s, began searching for a place to house this strange new capability—offensive cyberweapons—in the vastness of the military's combat commands.

From Rumsfeld's recently declassified "snowflakes"—his brief messages to his staff ordering up studies—it is clear that he sensed that cyberweapons were enormously powerful tools. But he struggled to understand how the Pentagon would use them. Naturally, the military had already developed jargon for the variety of techniques, vulnerabilities, and weapons in the arsenal. There were "computer network exploitation" operations, a fancy way of describing the theft of an adversary's data. And there were "computer network attacks," which are cyberattacks with real-world effects of the kind that were later tested in Olympic Games.

"Everything at the Pentagon needs a home," Hamre told me. "And Rumsfeld, rightly, saw this as a strategic weapon and gave it to Hoss Cartwright at Strategic Command."

Gen. James Cartwright, a marine aviator whose nickname, "Hoss," was taken from a character in the '60s television show *Bonanza,* ranked among the best strategic minds in a military consumed by the day-to-day battles in Iraq and Afghanistan. He walked around Strategic Command with a low-key demeanor and a crinkly smile, an everyman look from his days growing up in Rockford, Illinois. Cartwright had been pre-med and a competitive swimmer at the University of Iowa and, in the last days of the Vietnam War, signed up with the marines as a naval aviator. There's no room for error when taking off from and landing on aircraft carriers, and those high stakes appealed to Cartwright's sense of precision. But he also learned that naval aviators can never look like they are sweating the details, even when there is only one chance to catch the cable that keeps a plane from plunging into the sea during a deck landing.

By the time Bush took office in 2001, Cartwright had developed a fascination with the promise, and the danger, of cyberweapons. In his quiet but intense fashion, he began questioning whether the systems and strategies the Pentagon had built up in the decades after World War II were sufficient to meet the challenges of the next fifty years. The answer seemed obvious to him.

Yet inside the Pentagon one could make a lot of enemies questioning whether the conventional weapons that had gotten us through Vietnam and two wars in the Gulf remained critical in an age in which

breaking into an industrial control network might be more important than fielding new tanks and bombers. "There were a lot of people in the Pentagon who found Hoss's questioning refreshing," one of the members of the Joint Chiefs who served with him said to me. "And there were a lot who found it threatening."

That was especially true as Cartwright took on his first major job as a marine general in 2004: head of the US Strategic Command in Omaha, Nebraska. There was no job where precision and a strategic view of the world mattered more. Strategic Command, known as Stratcom, is in charge of the nation's nuclear arsenal. During the Cold War, it was the first line of defense against a nuclear conflict with the Soviets and was responsible for maintaining and moving nuclear weapons, drilling its staff for every scenario under which they might be launched, and making sure that any order to use them was authentic and legal. The opportunities for error on a horrific scale were endless.

Cartwright looked at Strategic Command's arsenal and began to ask a big question: Are these really the weapons that will keep the nation safe in the next half century? There were safety issues: the nuclear arsenal was aging; missile silos were still using five-inch floppy disks. The missileers working inside the silos were dispirited; not only were their command posts damp and out of date, but staffers were running through mind-deadening procedures preparing for an order that would probably never come.

Cartwright was equally concerned about the strategic vacuum. America's reliance on nuclear deterrence was actually restricting a president's ability to deal with the kind of adversaries the United States was facing every day, from the Middle East to East Asia. Because the consequences and casualties of using a nuclear weapon were so huge that they were paralyzing, Cartwright began to think strategically about the new cyberweapons that Rumsfeld had put under his command. They presented a huge intellectual puzzle and, as Hayden remembered later, "Hoss was strangely underemployed at Stratcom." He began thinking about how cyberweapons could expand a president's choices after deweapons had limited them.

"The tools available to a president or nation in between diplomacy and military power were not terribly effective," Cartwright told the US Naval Institute in 2012. He had by then left military service and was only beginning to unspool his thinking on this problem. What American presidents needed, he believed, were more coercive tools that could back up diplomacy. And nuclear weapons did not serve that purpose. No adversary thought an American president would ever reach for a nuclear weapon, except if the survival of the United States were at stake.

In his years at Strategic Command, Cartwright later said, he kept looking for new technologies the military could actually employ and, preferably, exploit so that the United States could prevail in a fight without ever firing a shot. These cyberweapons were what he called "speed-of-light" weapons—repurposed "electronic warfare" weapons that could disable an adversary's communications or paralyze its defenses. Others were directed energy weapons, such as lasers. Unlike nuclear weapons, these could be used in a first strike.

More important, beyond the damage they could inflict in wartime, cyberweapons had a coercive power in peacetime. Cartwright talked about using these weapons "to reset diplomacy," or to force a country to realize that it had little choice other than agreeing to negotiate. When he gave his 2012 speech, Cartwright never once made reference to Iran, but he didn't need to do so. To anyone watching the world scene at the time—a moment when the United States was simultaneously preparing to negotiate with Tehran and to go to war with it—his meaning was obvious.

Soon after Rumsfeld handed cyberwarfare to Strategic Command, a skunk works of sorts popped up there, exploring what it would take to deploy these weapons, how they should be used, and how the military's role in marshaling them would be different from the NSA's role. Over time, what emerged from Cartwright's creation was a prototype of what today is the US Cyber Command, although then it existed largely on paper and was barely staffed.

In 2007, with wars still raging in the Middle East and South Asia,

Cartwright moved on to become vice chairman of the Joint Chiefs of Staff. It was a rough transition. He wasn't an Iraq veteran, a liability at a time that this distinction was cherished as a prerequisite for higher command. Tension developed between Cartwright and the chairman of the Joint Chiefs, Adm. Mike Mullen, and worsened over time. Despite challenges, it was from this post that Cartwright began to put America's cyber forces in action.

In January of that same year, 2007, the director of national intelligence, John D. Negroponte, presented Congress with the annual worldwide threat assessment, an exercise that the nation's top intelligence officials understandably despised. It forced them to rank—in public—the major threats to the United States, and often it was only an exercise in telling Congress what it wanted to hear. But as a snapshot of national fears and obsessions at any given moment, it was nonetheless revealing.

When Negroponte settled into the witness chair that January day, he opened with a blunt statement: "Terrorism remains the preeminent threat to the homeland." Senators nodded in agreement. Dig further into his report, however, and one fact leaped out: cyberattacks did not even make the list. They were totally absent.

Yet even then, the nation's intelligence chiefs knew well that the daily skirmishing among superpowers was, if anything, intensifying. Chinese attacks on American companies—including military contractors—were ramping up. By 2008, the year after Negroponte testified, Chinese hackers working for the People's Liberation Army were inside Lockheed Martin's networks, making off with plans related to the F-35, the world's most sophisticated, and certainly most expensive, fighter jet. Later that year they hacked the campaigns of Barack Obama and John McCain, rivals for the presidency. Lisa Monaco, who was running the national security division of the Justice Department at the time, remembers clearly the first time she met Obama's senior staff. "I went out

to explain to them that the Chinese were all over their system," she said with a laugh years later, when she was the Homeland Security Advisor at the White House and overseeing the effort to bolster the nation's cyber defenses.

But the true wake-up call came on October 24, 2008, with the nation on the brink of Obama's election. Debora Plunkett remembers it well. A month into a new job running the NSA's Advanced Network Operations division, she was assigned to develop and deploy tools to determine if anyone was inside, or trying to get inside, the US government's classified networks.

Plunkett hadn't taken a conventional route to the NSA. The daughter of a long-distance trucker, she had grown up not far from Fort Meade but had never heard of the agency until after college. Coming off two tough years in forensics with the Baltimore Police Department, she was advised by a friend's boyfriend who worked for the NSA to take the entrance exam. She was given only a vague description of the agency's work, but for Plunkett, who loved puzzles, what she heard sounded intriguing. She passed the exam and joined the NSA in 1984.

Over the next quarter century, Plunkett became one of the few African American women to rise within the NSA leadership. "I was quite often the only minority and absolutely the only minority woman in my workspace and organization," she said. She climbed from the cryptography section to her position running the ANO and soon found herself leading a search for network intruders.

On a brisk fall day at Fort Meade in 2008—just ahead of Obama's election—Plunkett's team found something that made her blood run cold: Russian intruders in the Pentagon's classified networks. This was a new encroachment for the defense department, which had never—until that moment—discovered a breach in what was known as SIPRNet (it had the unwieldy name of "Secret Internet Protocol Router Network"). SIPRNet was far more than an internal network: It connected the military, senior officials in the White House, and the intelligence agencies.

In short, if the Russians were in that communication channel, they had access to everything that mattered. Plunkett recalls that "pretty soon we went straight to Alexander," meaning Gen. Keith Alexander, then the director of the NSA.

Investigators raced to figure out how the Russians had gotten inside. The answer was pretty shocking: The Russians had left USB drives littered around the parking and public areas of a US base in the Middle East. Someone picked one up, and when they put the drive in a laptop connected to SIPRNet, the Russians were inside. By the time Plunkett and her team made their discovery, the bug had spread to all of US Central Command and beyond and begun scooping up data, copying it, and sending it back to the Russians.

It was a bitter lesson for the Pentagon—they were, in fact, easy pickings for attackers using a technique that the CIA and NSA had often used to get into foreign computer systems. "People worked through the night to come up with a solution," Plunkett recalled. "We were able to develop what we thought was a reasonable solution that ended up being a very good solution." The fix—called Operation Buckshot Yankee—was deployed by the Pentagon later that day. Then, to keep a similar breach from happening again, USB ports on Department of Defense computers were sealed with superglue.

But the damage had already been done. As William Lynn, then deputy secretary of defense, later explained, the intrusion "was the most significant breach of U.S. military computers ever, and it served as an important wake-up call."

Perhaps so, but not everybody woke up. After leaving the NSA, Plunkett told me that for all her efforts—and they were considerable—she remained amazed by how easily outsiders appeared able to break into government and corporate systems. With every major hack, "folks like me will say—this will be the moment, this is the watershed moment. And it never was," she added, "because we're so lax about security and so inconsistent in investing in security.

"We just make it easy for them."

. . .

While Plunkett was trying to fortify the Pentagon's networks against the Russians, the NSA's offensive team, working not far away on the Fort Meade campus, was already making centrifuges blow up in Natanz.

Prodded by General Cartwright, Keith Alexander at the NSA, and a range of other intelligence officials, President Bush had authorized a covert effort to inject malicious code into the computer controllers at the underground Iranian plant. Part of the plan was to slow the Iranians and force them to the bargaining table. But an equally important motivation was to dissuade Prime Minister Benjamin Netanyahu of Israel from bombing Iran's facilities, a threat he was making every few months. Bush took the threat very seriously. Twice before the Israelis had seen threatening nuclear projects under way, one in Iraq, the other in Syria. They had destroyed them both.

Olympic Games was a way to keep the Israelis focused on crippling the Iranian program without setting off a regional war. But getting the code into the plant was no easy task. The Natanz computer systems were "air gapped" from the outside, meaning they had no connections to the Internet. The CIA and the Israelis endeavored to slip the code in on USB keys, among other techniques, with the help of both unwitting and witting Iranian engineers. With some hitches, the plan worked reasonably well for several years. The Iranians were mystified about why some of their centrifuges were speeding up or slowing down and ultimately destroying themselves. Spooked, they pulled other centrifuges out of operation before those met the same fate. They started firing engineers.

At Fort Meade, and the White House, the subterfuge seemed successful beyond anything its creators had hoped. And then all went wrong.

No reporter or news organization exposed Olympic Games. The governments of the United States and Israel managed to do so all by

themselves, by mistake. There has since been a lot of finger-pointing about who was responsible, with the Israelis claiming the United States moved too slowly, and the United States claiming the Israelis became impatient and sloppy. But one fact is indisputable: the Stuxnet worm got out into the wild in the summer of 2010 and quickly replicated itself in computer systems around the world.

It showed up in computer networks from Iran to India, and eventually even wound its way back to the United States. Suddenly everyone had a copy of it—the Iranians and the Russians, the Chinese and the North Koreans, and hackers around the globe. That is when it was given the name "Stuxnet," a blend of keywords drawn from inside the code.

In retrospect, Operation Olympic Games was the opening salvo in modern cyber conflict. But at the time, no one knew that. All that could be said for sure was that a strange computer worm floating around the world had emanated from Iran, and in that summer of 2010 Iran's nuclear program seemed a natural target.

In the newsroom of the *Times*, we had been on high alert for any evidence that a cyberweapon, rather than bombs and missiles, was being aimed at Iran's nuclear complex. In early 2009, just as Obama was preparing to take office, I reported that President Bush had secretly authorized a covert plan to undermine electrical systems, computer systems, and other networks on which Iran relies, in the hopes of delaying the day that Iran could produce a workable nuclear weapon. Eighteen months later, no one was surprised when evidence began to mount that Stuxnet was the code we had been looking for.

Soon an unbeatable team of cyber sleuths—Liam O'Murchu and Eric Chien of Symantec—grew intrigued. They were the odd couple of cyber defense: O'Murchu a boisterous Irishman with a thick brogue who raised the alarm at Symantec, and Chien the quiet engineer who dug in. For weeks the pair ground away at the code. They ran it through filters, compared it to other malware, and mapped how it worked. "It's twenty times the size of the average piece of code," but contained

almost no bugs, Chien recalled later. "That's extremely rare. Malicious code always has bugs inside of it. This wasn't the case with Stuxnet." He admired the malware as if he were an art collector who had just discovered a never-before-seen Rembrandt.

The code appeared to be partially autonomous; it didn't require anyone to pull the trigger. Instead, it relied on four sophisticated "zero-day" exploits, which allowed the code to spread without human help, autonomously looking for its target.* This fact provided a crucial clue to Chien and O'Murchu: such vulnerabilities are rare commodities, hoarded by hackers, and sold for hundreds of thousands of dollars on the black market. It became clear that Stuxnet couldn't be the work of an individual hacker, or even a team of hobbyists. Only a nation-state could have the resources—and the engineering time—to assemble such a sophisticated piece of code. "It blows everything else out of the water," O'Murchu told me later.

Unsurprisingly the two men grew paranoid about who might be watching them as they watched the code. Half joking, Chien told O'Murchu one day, "Look, I am not suicidal. If I show up dead on Monday, you know, it wasn't me."

Stuxnet's inner workings harbored another clue that Iran's nuclear program was the malware's target. The worm seemed to be probing for something, in this case a specific kind of hardware known as a "programmable logic controller" made by Siemens, the German industrial giant. These are specialty computers that control water pumps, air-conditioning systems, and much of what happens in a car. They turn valves on and off, control the speed of machines, and watch over an array of sophisticated, modern-day production operations: In chemical plants, they control the mix. In water plants, they control fluorination and flow. In power grids, they control electricity. And in nuclear enrichment plants,

* A zero-day flaw is a previously unidentified software vulnerability—so named because there are zero days of notice to get it fixed before the damage is done.

they control the operation of the giant centrifuges that spin at supersonic speeds.

Chien and O'Murchu began publishing their findings in the hope that someone out there was expert in the kind of systems this strange code seemed to be targeting. Their plan worked. One expert in Holland explained to them that part of the code they had published was searching for "frequency converters," devices used to change an electric current, or sometimes change the voltage.

There aren't many innocent explanations for sneaking into someone's infrastructure to change the flow of an electric current. And in Iran's nuclear facility at Natanz, frequency converters played a critical role: they were part of the control system for nuclear centrifuges. And the centrifuges, the US government's experts knew from their own bitter experience, were highly sensitive. Because they spun at supersonic speeds, any dramatic change—triggered, say, by a change in current—could send the rotors out of kilter, like a child's wobbling top. When they became unstable, the centrifuges would blow up, taking out any machinery or people nearby. Uranium gas would be spilled all over the centrifuge hall.

In short, to stop the Bomb, America's new cyber army had made a bomb—a digital one.

As Iran's centrifuges were spinning out of control, the operators at Natanz had no idea what was happening. The data that showed up on their screens seemed normal—the speed, the gas pressure. They had no way of knowing that the code was faking them out and suppressing the signs of imminent disaster. By the time the operators figured out something was dangerously wrong, they could not shut down the system. The malware had affected that process too.

There were other clues. Although the malware eventually infected computers around the world, it kicked into gear only when it found a very specific combination of devices: clusters of 164 machines. That number sounded pretty random to malware sleuths, but it set off my mental alarms. The centrifuges at the Natanz nuclear facility—I [illegible] of covering Iran's nuclear program and interviewing

inspectors from the International Atomic Energy Agency—were organized in groups of 164.

That left little mystery about the intended target.

The following summer and fall, two *Times* colleagues, Bill Broad and John Markoff, and I published several stories about the hints emerging from the Stuxnet code. Markoff uncovered stylistic and substantive evidence of Israel's role in the code writing. Next, we found one of several American calling cards embedded in the code—an expiration date, when the code would drop dead. Teenagers don't put expiration dates into their code. Lawyers do—for fear that malware could become the digital equivalent of an abandoned land mine in Cambodia, waiting for someone to step on it two decades after it was planted. Finally, Bill Broad discovered the final clue we needed: evidence that the Israelis had built a giant replica of the Natanz enrichment site at their own nuclear weapons site, Dimona. (We didn't yet know the United States was doing the same thing in Tennessee.) The purpose was clear: both countries were building models to practice their attacks, much as the United States built a model of Osama bin Laden's house in Abbottabad, Pakistan, around the same time, to practice the impending raid against the world's most wanted terrorist.

In mid-January of 2011, we felt we had enough information to publish our first story about who had been behind the Stuxnet attacks. In a Sunday article, we laid out the compelling evidence that the United States and Israel had produced the malware together in order to slow Iran's nuclear progress. The story was full of details and markers that took the code right to the gate of Fort Meade, where the NSA is located, but upon publication there was no political outcry, no investigation. That would come more than a year later.*

But even after we published our account it was clear there were

---

* The reason for the delay may lie in a coincidence of timing. That first big story was published just hours before Egypt erupted into the chaos of the Tahrir Square uprising, which then occupied all the headlines, and forced President Obama into a tense effort to get President Hosni Mubarak to leave office.

major questions left unanswered: Had this been a small operation gone awry, or a large, well-hidden effort? Assuming the United States and Israel had combined forces to design this enormously complex cyber-weapon, who had given the go-ahead? After all, we knew that in the United States only the president could authorize offensive cyber action, just as he had to provide the launch codes for nuclear weapons.

And if Olympic Games was a sign of where American covert action was headed, were we ready as a nation to open this Pandora's box? Once opened, could it ever be closed again?

THE DISCOVERY THAT Israel had built a replica of the Natanz plant drove home how central a role the Israelis had played in developing the Stuxnet malware. The more sources I interviewed, the more it became clear that the cyber program widened a divide between Prime Minister Benjamin Netanyahu and his brilliant, short, bald spymaster, Meir Dagan. In Dagan's younger days in the Israeli military, he had led squads that hunted down Palestinian militants. Ariel Sharon, the Israeli prime minister who had been Dagan's commander and mentor, famously if crudely declared that "Dagan's specialty is separating an Arab from his head." It was a brutal description, even in the macho world of the Mossad, Israel's best-known intelligence agency, which Dagan ultimately led for nine years—an extraordinarily long tenure. While Dagan pretended to dismiss the stories as mythmaking, he nonetheless seemed to revel in them.

But the mythmaking ignored the fact that it wasn't only Arabs whom Dagan had in his sights. Many observers suspected Dagan's hand in the killing of Iranian nuclear scientists, who were assassinated while driving to work in Tehran traffic after motorcyclists pulled up and attached "sticky bombs" to their car doors before speeding off. If Dagan were indeed behind the killings, it would be in keeping with his view that an Iran armed with a nuclear weapon was truly an existential threat to Israel. Indeed, to talk to Dagan for five minutes was to discover a man who viewed the world through the lens of the Holocaust. On his desk, he kept a photograph of his grandfather kneeling on the ground before his Nazi captors moments before he was killed. It was Dagan's personal "never again" memento that seemed to explain the determination with which he organized the elimination of Israel's enemies.

Dagan made no secret that he never hesitated to send Mossad agents out to kill. Yet when one of those missions went bad—his agents were caught on tape entering and leaving a hotel in Dubai just before and after the 2010 killing of a senior official of Hamas, the Islamist Palestinian group—it was the beginning of the end of his career. The images of the Israeli agents, dressed casually in tennis gear as they entered and left the hotel, played again and again on television. But as his time as the chief of the Mossad dwindled down, Dagan wanted to be remembered instead for managing an operation that was, in his mind, a complete success: the malware attack that crippled Natanz.

Despite Dagan's public reputation as a brutal spymaster who had killed many Arabs in his younger days and ordered the deaths of many more from Mossad headquarters, he was far more strategically savvy than most Israelis knew. Internally, he was increasingly vocal that bombing Iran was madness—it would simply drive the nuclear program further underground. That program would then come back, bigger and more advanced than before. Dagan devoted his last years in office to dissuading Prime Minister Netanyahu from an air attack. "The use of [military] violence would have intolerable consequences," Dagan later told Israeli investigative journalist Ronen Bergman. "If Israel were to attack, Khamenei would thank Allah," he said, referring to the Iranian Supreme Leader. "It would unite the Iranian people behind the project and enable Khamenei to say that he must get himself an atom bomb to defend Iran against Israeli aggression."

All of which meant that by 2010 Dagan was under tremendous pressure to show Netanyahu that a more covert, more sophisticated approach to crippling the Iranian program could succeed.

Dagan and I never met when he was in office. But I was determined to change that after I heard that at one of his retirement parties many of the toasts and jokes made oblique references to the cyberattacks on Natanz. The insiders got the drift; others were left to wonder what everyone else was laughing about.

We first talked in 2011 a few months after Dagan had been ousted from his job by Prime Minister Netanyahu. It was clear he was still bitter about his ouster. He variously derided Netanyahu as a terrible manager and an incompetent warrior. Rightly or wrongly, Dagan believed that Netanyahu had gotten rid of him because the Mossad chief, like other Israeli intelligence leaders, opposed efforts by the prime minister to bomb Iran's nuclear facilities.

"Bombing would be the stupidest thing we could do," Dagan told me. This was not like striking Iraq's Osirak nuclear reactor in 1981 or Syria's reactor in 2007. He believed Iran's program was simply too sprawling; they were not about to repeat their neighbors' mistakes. So while an air attack on Iran's facilities "might make me feel good," Dagan said to me one afternoon, it would provide an illusory solution. The satellite photographs, he said, would show Iran's facilities flattened, and everyone would cheer. But within months, he predicted, those facilities would be rebuilt so deep as to be impermeable to a second strike. And that, he thought, would be disastrous for the state of Israel.

It was fine to try to slow Iran's progress, said Dagan. But if Israel attempted to destroy the country's nuclear facilities in an overt attack, it would ensure a nuclear Iran. There had to be a better way.

A cyberweapon, in his view, was the way out of the conundrum. In our early meetings, Dagan was coy about his role in the development of Stuxnet, even when I mentioned that I had heard about his participation in secure videoconference debates about next steps in the attacks. He didn't know much about computers, he often replied to me with a smile, as if that exonerated him from the role we both knew he played.

Yet over time, as he grew sicker from a failing liver transplant, he

edged closer to describing what happened, and why. In our handful of conversations over the years, he sprinkled phrases like "if we did it" into many sentences so that he could explain his underlying logic without violating his oath to maintain the secrecy around the Mossad's covert operations. He talked about how Israel's technology made it enormously difficult for the Iranians to figure out the origin of the attack. The operation against Iran was a model of how Israel should defend itself in the future, he said. Gone were the days of open demonstrations of military might that invited retaliation, escalation, and international condemnation. Gone were the days of occupying territory. The defense of Israel, he insisted, required subtlety and indirection.

"I doubt he knew the first thing about how you write a string of code," one American who dealt with Dagan often told me. "But he knew a lot about how you play with an enemy's mind." And he was convinced that it was the intelligence services that would end Iran's nuclear program, not the air force. It was a mind-set that put Dagan and Cartwright in the same place. And many of Dagan's fellow intelligence chiefs, once they left office, claimed they backed his arguments.

I never heard Dagan directly admit his role in the cyberattacks. But he hinted they had been designed as much to divert Netanyahu from stumbling into a Mideast war as to stop the Iranians from enriching uranium. "I don't trust him," Dagan said of Netanyahu. It was in Netanyahu's interest, he told me, to portray the Iranians as irrational zealots who would use their bomb against Israel. But Dagan looked at the Iranians and saw a group of mullahs mostly interested in staying in power, rather than starting a suicidal war.

There was a reason, Dagan told me, that Bush would not give the biggest bunker-busting bombs to Netanyahu. "He was afraid Bibi would use them," Dagan told me. "And so was I."

That fear explained Dagan's enthusiasm for using cyberweapons against Tehran. It was a way to set the nuclear program back. Perhaps more important, Bush and Obama were able to argue to Netanyahu that there was no reason to bomb while the cyberattacks were working.

The last time I saw Dagan, he chewed me out for what I had written about Olympic Games. But unlike his American counterparts, he complained that I had written too little, not too much.

"You missed a major part of the story," he said, arguing that the Americans had received far too much credit, and the Israelis—and by extension Dagan himself—had received not nearly enough. I had been seduced by Americans who were intoxicated with advertising their own success, he insisted one evening, rather than giving credit to an ally—he carefully didn't say which one—that had done the heavy lifting, gotten the code into the centrifuges, and revised it as necessary.

I would be happy to tell more of Israel's side of the story, I told him, but he'd have to be more explicit about the operational details to prove his point. He smiled—a smile of disgust.

"I am an old man," he said, "and I am sick. I don't want to spend my last days in jail."

BY THE END of 2011, after dozens of interviews, I had pieced together the highlights of the story of the strategy and debates swirling around the decision to unleash Stuxnet—or at least as many of them as I could gather, given the layers upon layers of secrecy involved. After consulting editors, and the *New York Times* in-house counsel, it was time to go to the Obama White House to see if they were ready to talk—both about what had happened and about any national security concerns they might have about publishing the details. As in all such cases, I made clear that the *Times,* and the *Times* alone, would decide what to publish. But if there were risks to ongoing operations or lives, we needed to discuss them now, not after publication.

My first visit was to Benjamin Rhodes, the former novelist and graceful speechwriter who eventually handled a portfolio of diplomatic issues for Obama, including the opening of Cuba. It was his job to deal with reporters who came to the administration with complex, sensitive national security stories and to decide how, if at all, the White House would respond. Without getting into the details of what happened, he suggested that I go see General Cartwright. It made sense, since Cartwright's term in office spanned the Bush and Obama administrations, and he had been at the center of all offensive cyber debates and understood their sensitivities. Cartwright had retired from the marines after he was passed over for chairman of the Joint Chiefs in 2011 and knew the history of the US military's development of a cyber arsenal better than anyone else.

I knew Cartwright from his days on the Joint Chiefs and had attended conferences where he had discussed the strategic challenges of the new age of cyber conflict. In my reporting on Olympic Games, his name came up often as the man who had tutored Obama about how the Stuxnet worm worked (though it had not yet been given the name "Stuxnet") and rolled out the "horse blanket" diagram of Natanz to bring Obama up to date.

But Cartwright's direct line to Obama had grated on Robert Gates, the secretary of defense, and Mike Mullen, the chairman of the Joint Chiefs. On a variety of issues they believed he manipulated the Pentagon system, or went around the chain of command. It didn't help that Cartwright had not spent time in Iraq and Afghanistan. When Mullen was ready to retire, the two successfully argued against promoting Cartwright into Mullen's role. Suddenly, the man who was among the first to sketch out how the United States could create a dedicated military command to deal with a new dimension of warfare was cast out. With him, I discovered later, went some of the most creative strategic thinking about the use of cyber in offense and defense.

Since retiring, Cartwright had taken a chair at the Center for Strategic and International Studies and signed on with a handful of defense firms, including Raytheon, the maker of missile defenses and defense electronics. Carefully, he had begun to speak out against the secrecy surrounding America's new cyber arsenal, arguing that if the United States wanted to create cyber deterrence it was going to have to show a bit of its capability. "You can't have something that's a secret be a

deterrent," I heard him say in more than a few public forums. "Because if you don't know it's there, it doesn't scare you."

He was right, and with the utmost care, the Pentagon began to slip a few lines into public testimony acknowledging that it possessed offensive cyber capabilities. It was a little like acknowledging that the sun rose in the morning. Still, it wasn't an enormously welcome message in the intelligence world, which feared a slippery slope toward divulging what those weapons were and how they were used. Meanwhile, Cartwright was also making a case that the United States could survive quite nicely, thank you, with far fewer nuclear weapons—an argument that carried extra weight coming from the former head of Strategic Command. Again, he was right. But his argument didn't exactly win him friends among his old Pentagon colleagues, who rarely met a weapons system they didn't like.

I took Rhodes's advice and called Cartwright. By the time I went to see him, I not only knew the outlines of the story about Olympic Games, I had already drafted them into two chapters of a book about Obama's first term, describing Olympic Games in as much detail as we could dig up at the time. The book was due to be released in months, and the manuscript was already being edited. That fact became significant later on, when the FBI—whose special agents must have never encountered a book-production schedule before—wrongly concluded that Cartwright was the source of the tale.

My goal in seeing Cartwright was twofold: to check that I had the history and implications right, and to get an independent view of whether any details I was reporting could jeopardize American national security. Cartwright knew that I had been sent by the White House, and saw himself as part of the effort to dissuade me from publishing any details of the operation that might aid an American adversary. He made it clear that he could not discuss classified details. Yet as it turned out when the FBI went looking for a "leaker"—as if there were a single one—we were both a little naïve. For doing what he thought was right, he later paid an awful price, for which I feel enormously guilty to this day.

. . .

It was just a few days later that I made my trek out to the CIA headquarters to visit Michael Morell in his seventh-floor office—surrounded by three decades of memorabilia from his career, including artifacts from the raid that killed Osama bin Laden. Morell was close to President Obama, and I knew that if the administration was going to push back against the story, he would be the man to do it.

We began pacing through my reporting and the story I was preparing to tell. I ticked through the forensics that led experts to identify the United States and Israel, the carcasses of blown-apart centrifuges found by international inspectors, the mock-ups of Natanz built by the Israelis at Dimona and by the United States in Tennessee. I described the Situation Room debates in which Morell participated. He cautioned against a few assertions and argued with a few conclusions. At a few moments in the story he slowed down, taking notes and suggesting that he might ask that I remove references to certain techniques that the agency used to get malware into target computers and networks. (Curiously, a few weeks later, he asked that a reference to one of those techniques be restored. Though he offered no explanation, clearly the agency had moved on to other methods and wanted to keep the Iranians thinking that the old techniques were still in use.)

In the end, Morell asked for only a handful of deletions, mostly technical details that focused on how the United States put "beacons" and malware into foreign systems and networks. None was essential to telling the story of the most sophisticated state-sponsored cyberattack in history. "You agreed to just about everything we asked for," he acknowledged later on, even while still objecting to the fact that we were publishing anything at all about an American covert operation.

But none of that mattered when the story was published. Republicans who were trying to cast Obama as weak on terrorism—not easy after the killing of bin Laden—accused the White House of leaking the story, along with an unrelated story in the *Times* about the president's role in approving a "kill list" of terrorists to be targeted by drones.

"We know the leaks have to come from the administration. And so we're at the point where perhaps we need an investigation," said Sen. John McCain. He called the story part of "a pattern in order to hype the national security credentials of the president and every administration does it. But I think this administration has taken it to a new level."

Obama himself performed a delicate dance: He couldn't confirm the story, of course, or deny it, but he wanted the world to know he wasn't the source. "I'm not going to comment on the details of what are supposed to be classified items," he said with a hardness in his voice a few days after the details about the White House origins of Olympic Games were published. "When this information, or reports, whether true or false, surface on the front page of newspapers, that makes the job of folks on the front lines tougher and it makes my job tougher—which is why, since I've been in office, my attitude has been zero tolerance for these kinds of leaks and speculation.

"Now, we have mechanisms in place where if we can root out folks who have leaked, they will suffer consequences. In some cases, it's criminal." He quickly added: "The notion that my White House would purposely release classified national security information is offensive. It's wrong."

His comments, made in June 2012, underscored the reflexive secrecy surrounding all things cyber, particularly odd in this case because the code had been spreading around the globe for two years. They also essentially forced the Justice Department to launch a leak investigation, which Attorney General Eric Holder announced around the same time. The White House chief of staff ordered all employees to preserve any notes or emails or communications with me. Since I had been covering the Obama national security team for more than three years, there were a lot of those. Soon the FBI began interviewing scores of potential witnesses. They obtained a secret warrant to get all the emails sent and received by General Hayden, the former CIA and NSA chief. And they used the CIA's notes from my conversation with Morell to try to point the finger at General Cartwright. Why [illegible] picked him, out of the scores of officials in the United States and

abroad whom I interviewed, remains a mystery to me. (At one point they came to him with highlighted lines he had used in speeches, and the syntax of paragraphs I had written, looking for commonalities. Of course, all quotations were from Cartwright's public, on-the-record, unclassified statements.)

As Cartwright himself has since acknowledged, he made an error of judgment in agreeing to be interviewed by the FBI without a lawyer present; he said he thought they were all on the same side. When the interview with the FBI became confrontational, the complaint filed in his case reported, he became ill and was briefly hospitalized. Later, when he was indicted, it was for lying to the FBI about when and how we had met.

He was never charged with leaking any classified information. And as far as I can tell, he never did. But that crucial fact almost didn't seem to matter.*

The supreme irony of the Cartwright case is that the man who'd helped propel the federal government into shaping a sophisticated approach to dealing with the world's most complex weapon was among the first victims of the paranoia about discussing that approach. The government could have responded to the disclosures about Olympic Games by embracing the revelations and reminding adversaries—Iran, Russia, and North Korea among them—that the United States could do far worse to them. It could have explained why cyber was critical to avoiding a shooting war in the Middle East. It could have used the moment to talk about what kind of global rules we should create for using cyberweapons against civilians, against commercial facilities, and against other governments.

The government did none of that. The Pentagon and the intelligence agencies were unwilling to discuss publicly how they might limit the use of cyberweapons, in times of both war and peace.

Partly that reluctance reflected the fact that the United States still

---

* In 2016, Cartwright pled guilty. Obama gave him a full pardon in the last days of his presidency, even restoring his security clearances.

believed it had a lead, if a narrowing one, in cyber technology. In the early days of the nuclear age, many officials had opposed even a discussion of arms control, arguing that there was no reason for the United States to shorten a long lead over its competitors. (The first limits on nuclear weapons happened in the early 1960s, only after the Soviets had a full arsenal, and Britain, France, and China were building them.) But the silence and obsession with secrecy may have had a deeper motivation: American intelligence services had a menu of other cyber operations brewing around the world. These ranged from classic espionage to highly destructive malware—the kind that could knock a whole country back into the analog age.

CHAPTER II

PANDORA'S INBOX

The science-fiction cyberwar scenario is here. That's Nitro Zeus. But my concern, the reason I'm talking, is when you shut down a country's power grid, it doesn't just pop back up. It's more like Humpty-Dumpty. And if all the king's men can't turn the lights back on, or filter the water for weeks, then lots of people die. And something we can do to others, they can do to us too. Is that something that we should keep quiet? Or should we talk about it?

—An NSA employee, speaking through a composite character in Zero Days

After the Russian hack of the Pentagon's secret networks in 2008, two things seemed clear to the newly inaugurated Obama administration. First, Putin's hackers were sure to come back. And second, America needed a full-fledged Cyber Command, far more capable than the small units spread among the army, the navy, the air force, and Cartwright's Strategic Command. It was time for a true military organization, with its own troops, that integrated digital offense and defense.

But no one was quite sure what that digital army was supposed to look like, or how it would wage war. Politicians instantly grasped all the other battle "domains": land, sea, air, space. They could picture conventional equipment like tanks, aircraft carriers, bombers, and satellites. But cyber, as Keith Alexander, then the head of the National