Chapter 8

Olympic Games

When the centrifuges first began crashing in 2008 at the Natanz enrichment center, the crown jewel of the Iranian nuclear program, the engineers inside the plant had no clue they were under attack. That was exactly what the designers of the world's most sophisticated cyberweapon had planned.

The idea, hatched in Washington and Jerusalem, was to make the first breakdowns seem like random accidents and small ones at that. A few centrifuges—the tall, silvery machines that spin at the speed of sound to purify uranium—raced out of control, seemingly for no reason. With a little luck, they would blow apart, forcing the Iranians to shut down the whole plant and spend weeks figuring out what went wrong.

"The thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence," one of the architects of the earliest attacks told me later. A mechanical failure seemed entirely plausible. Iran purchased its centrifuge designs from A. Q. Khan, the rogue Pakistani who sold himself as the father of the Pakistani bomb, to speed their ability to make enriched uranium. In fact, the evidence suggests it set them back by years. The design he peddled, called the P-1 for Pakistan's first attempt at a centrifuge, was so deeply flawed that even the Pakistanis stopped using it years ago. The P-1s had developed a reputation over the years as the Ford

Pintos of the nuclear world, subject to periodic, random explosion. Bad ball bearings could cause a catastrophic failure. So could a tiny blip in the electrical system. But the Iranians were determined to keep them running until they could design and build a better one on their own.

A few weeks would go by and then there would be another breakdown—and then another. Each seemed to be caused by a different flaw. And that, too, could be easily explained: fearing inspectors and foreign plots, Iran's nuclear engineers had spread the work of assembling the machines to scores of small shops, where they could be easily hidden. Secrecy was vital; no one in Tehran wanted to repeat the embarrassment they suffered years ago, when IAEA inspectors found an entire assembly operation behind a false wall of a clock factory.

It was particularly difficult to manufacture the delicate rotors at the center of the machines. The rotors are the most vital single part: they spin at terrifying speeds, and each rotation of each centrifuge creates a slightly more purified version of Uranium-235. But they are very temperamental. Spin them up too quickly and they can blow apart. Put on the brakes too fast and they get unbalanced. When that happens, the rotors act like a metallic tornado, ripping apart anything in its way—including any human beings unlucky enough to be working in the enrichment center at the time.

This was exactly the vulnerability that nuclear experts and computer engineers inside the United States and Israeli governments decided to try to exploit in 2007 and 2008. What if they could somehow secretly take command of the specialized computer controllers that run the sprawling centrifuge plant at Natanz? What if they could implant some code that would lie dormant for weeks or months, waiting for a chance to wreak havoc? And what would happen if one day, when the Iranians thought everything was running smoothly, the code would kick in to order those centrifuges to speed up too quickly or slow down too fast, creating exactly the

kind of instability that sometimes happens naturally? And how long would it take the Iranians to figure out that someone, somehow, had gotten inside their system?

Those questions ultimately led to the creation of one of the most secret, compartmentalized programs inside the US government. The details of "Olympic Games" were known only by an extremely tight group of top intelligence, military, and White House officials. The intent of the operation was twofold. The first was to cripple, at least for a while, Iran's nuclear progress. The second, equally vital, was to convince the Israelis that there was a smarter, more elegant way to deal with the Iranian nuclear problem than launching an airstrike that could quickly escalate into another Middle East war, one that would send oil prices soaring and could involve all the most volatile players in the region. "We told the Israelis that if you bomb Natanz, it will take the Iranians two years to replace it—but they will do so deep underground; you won't be able to get it the next time, and you'll make them want the bomb even more," one participant in the program told me. "But if you do it this way, they won't see it, and the longer we can go before you have to bomb it."

It was a brilliant theory. But no one knew whether it would work, or for how long. When President Bush held his one-on-one meeting with President-elect Obama days before the transfer of power in early 2009, he told him the program could mean the difference between peace and war with Iran. Obama, at first, may have had his doubts. But he did know that it would be the most dramatic field test in history of a new weapon in America's arsenal—a weapon that of course could, sooner rather than later, be turned back on the United States.

"THE MOST ELEGANT cyberattacks are a lot like the most elegant bank frauds," one of the early architects of Olympic Games told me in 2011, as I began to delve into the question of how Washing-

ton was making use of a new technology—offensive cyberweapons—which it spends billions of dollars on each year and steadfastly refuses to talk about.

"They work best when the victim doesn't even know he's been robbed."[1]

The origins of the cyberwar against Iran goes back to 2006, midway through George W. Bush's second term. Bush had often complained to his secretary of state, Condoleezza Rice, and his national security adviser, Stephen Hadley, that his options regarding Iran looked binary: let them get the bomb or go to war to stop it.

"I need a third option," Bush told them repeatedly.

When that option emerged, it came from inside the bowels of the US Strategic Command, which oversees the military's nuclear arsenal. Since its creation, the command has focused almost exclusively on how to improve and defend "the triad"—nuclear weapons based in silos in the United States, in bombers that carry the weapons, and aboard the "boomers" of America's submarine fleet. But it became increasingly evident to the general commanding those strategic forces, James Cartwright, that these weapons of the past were of little utility in the kinds of conflicts the United States found itself in today. That was equally evident to Mike McConnell, the last director of national intelligence under Bush. Cartwright set up a small cyber unit within his operation that later blossomed into the United States Cyber Command, which now is the centerpiece of the Defense Department's offensive cyber capability. McConnell, meanwhile, worked to build up the capacity of the National Security Agency, the huge intelligence agency that has a lock on much of the government's best offensive cyber talent.*

So both at the sprawling nuclear command base in Nebraska

* US Cyber Command is based at Fort Meade, Maryland, so that the Defense Department's operations are alongside those of the NSA. Gen. Keith B. Alexander, who is the director of the NSA, is also the commander of what the Pentagon calls USCYBERCOM.

and inside the NSA's headquarters at Fort Meade, Maryland, the United States began thinking in detail about how cyberweapons might be used against the infrastructure of another nation—grinding its machinery, its electric power systems, or its markets to a halt.

It was an entirely new territory for the Defense Department, which for the first time in decades was thinking about a weapons system it didn't know how to build. And while cyber issues are hardly new to the NSA, its mission was to collect intelligence, not fight wars or execute covert actions. Naturally, turf wars broke out at various agencies in Washington over who should be responsible for cyber offense and cyber defense—a battle that has never been fully resolved.

But the Iran problem would not wait. In 2006, Iran resumed the uranium enrichment at Natanz after negotiations with the Europeans and the United States floundered. President Mahmoud Ahmadinejad made no secret of the country's plans: he took Iranian reporters on a tour of Natanz and described grand ambitions to install upwards of fifty thousand centrifuges. For a country that had only one nuclear reactor—whose fuel came from Russia—it seemed hard to justify as a civilian energy project. For years to come, Iran would have no place to burn the reactor fuel it is spending billions to produce. But the fuel's other utility—if it was ever enriched to bomb grade—seemed obvious.

The solution that Cartwright and others presented to Bush, Hadley, and Rice was straightforward: buy some time to deal with the Iranian nuclear program by, in the words of one senior intelligence official, finding new ways "to throw a little sand in the gears." No one had high expectations. The United States had only attempted relatively minor cyberattacks before, for example on an al-Qaeda cell in Iraq—nothing very sophisticated. If this plan worked, they thought, perhaps it could slow the Iranian program by a year or so. Along the way, the United States would learn about this new form of weaponry. But Rice and Hadley, in particular, saw Olympic Games as the best bet to forestall an Israeli attack. They saw no other

option: when they asked the CIA to bring them, one more time, the array of "kinetic options"—physical attacks on Iran's facilities from the air or the ground—none of them looked workable. "It was a very short conversation," one participant in the review said later.

Bush immediately seized on the cyber idea and issued the orders to allow it to go forward. "It took us about eight months [to put together the first plan]," one of the key players told me, much of it spent with lawyers trying to make sure that the code they were writing did not violate the laws of armed conflict. The cyberattack had to be as accurate as the best guided missile—it couldn't take out hospitals or schools; it had to be focused on Iran's centrifuge plants. It had to be stealthy, leaving no "fingerprints." And somehow, it had to get inside the heavily guarded Natanz facility.

Soon, an attack plan was developed that bore little resemblance to any that past generations of military planners had ever taken through the northwest gate of the White House. The first step was to develop a bit of computer code called a "beacon" that could be inserted into the computer systems at Natanz to map their operations and determine how they controlled the centrifuges. Eventually the beacon would have to "phone home"—literally send a message back to the NSA's headquarters that would describe the structure and daily rhythms of the enrichment plant. The most important task would be to understand how the centrifuges were connected to what are called "programmable logic controllers"—specialized computers that run the fast-spinning machines, guiding their speed and controlling every aspect of their operation. The good news for the American cyberwar strategists was that these controllers are virtually undefended; like the first personal computers, they were designed in an era when no one ever thought that they might come under attack. They carried no virus protection, not even something as simple as Norton 360. As the designers of the attack knew, if they could get inside the controllers, they would likely have free rein to take control of them.

But getting in, and getting out again, required thinking a bit like a bank thief casing a well-protected vault. While there were few electronic protections, there were plenty of physical protections around Natanz, and a lot of paranoid Iranian officials who knew that their centrifuges were the target of saboteurs from the West. They knew from bitter experience.

OVER THE YEARS the Iranians had been the subject of repeated sabotage—but almost all of it was conventional stuff, the kind of industrial trickery that the CIA had specialized in from the earliest days of the Cold War. Nearly a decade ago, the United States and others had tinkered with power supplies sent to Iran from Turkey; when the equipment was installed at Natanz, an unstable electrical wave surged through the delicate centrifuges and caused them to blow up. It didn't take the Iranians long to figure it out and find another supplier. Gholam Reza Aghazadeh, one of the more hapless previous chiefs of Iran's nuclear program, implored his workers, "Build these machines even if they explode ten times more."[2]

After the Iranians caught on to the power-supply trick, the United States turned to inserting small defects into Iran's supply of critical vacuum pumps. The pumps were secretly diverted to the Los Alamos National Laboratory in New Mexico—home of America's first secret nuclear program—for "improvement" before they were delivered to the Iranians. And the list went on.

It had already occurred to the Iranians that the computer systems running the centrifuges at Natanz were huge targets. But they solved that problem in the same naïve way that many American corporations, power stations, or even the US military once relied on in a more innocent age: they made sure to not connect them to the Internet. Instead, they were surrounded by what engineers call an "air gap," meaning that the only way to get at the computers was to get inside the plant and work on them directly.

So the first challenge was to leap the gap. And the second was to implant the beacon.

It quickly became evident to the Bush administration that if the mission was going to be successful, the Israelis had to be involved—both to leverage their technical expertise, which rivaled the NSA's, and to take advantage of their intelligence about operations at Natanz. The Israelis would also have to be convinced that the new line of attack was working—and that the threat of airstrikes could be put off. Soon the American and the Israeli intelligence partnership kicked into high gear. Olympic Games became part of the weekly conversation between security officials from the two countries, conducted over secure video lines and with visits to Washington and Jerusalem.

"This was really unusual, because you have two intelligence agencies that don't usually play well with others," said one former American intelligence official who had worked extensively on Iran. But current officials dispute that, saying that Iran has brought American and Israeli intelligence and defense officials closer together than at any time in their history. And while "the bug," as some of the Americans called it, was first designed by a small cell of cyberwarriors at the National Security Agency, soon there were improvements, and new versions, coming out of Israel's famed Unit 8200, the country's NSA equivalent.*

Where the Israelis could also contribute, in the eyes of the Americans, was in penetrating the Iranian scientific community. As the assassinations, defections, and a flow of documents had made evident, the Israelis had informants deep inside some of Iran's most critical nuclear and missile projects. That was essential because the only way the beacon, and ultimately the malicious software itself, would leap the air gap would be with the help of scientists, engineers, and others who had access to Natanz.

---

* In meetings between officials in Washington and Jerusalem, the unit handling the Israeli side of the attacks was just referred to as ISNU, for Israel Sigint National Unit.

"We had to find an unwitting person on the Iranian side of the house who could jump the gap," said one participant in the planning. Fortunately, he said, between Israeli and American intelligence agencies "we had a pretty good idea who was going in." Soon there was a list of targets, from the scientists who worked inside the program (some of whom were listed, in public, in the annexes to United Nations sanctions lists) to technicians from Siemens, the giant German electronics firm whose programmable logic controllers, conveniently, had been purchased by the Iranians, who wanted their centrifuges run by the best available technology.[3]

The trick was to get the beacon into those programmable logic controllers. The best way was on small thumb drives—which could be plugged directly into ports on the controllers—or on laptop computers. Frequently, the engineers at Natanz work on program updates on their laptops, and then connect them directly to the controllers. "That was our holy grail," one of the architects of the plan said. As it turned out, it didn't take long to jump the air gap. "It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand," one of the architects of the plan later told me.

It took months for the beacons to do their work and report home—complete with maps of the electronic directories of the controllers, and what amounted to blueprints of how the centrifuges spinning in the basement in Natanz were connected to their electronic control systems. According to one person involved, it helped that Siemens was maintaining the system every few weeks, updating the software. "Siemens had no idea they were a carrier," one official told me. (American officials insist that the United States steered clear of the Siemens engineers, for fear of jeopardizing their relationship with Germany's intelligence service. But those diplomatic niceties apparently did not stop the Israelis.)

Soon it was not an issue: the Iranians, suspicious of the German

engineers, banned them from access to Natanz, either directly or remotely.

With the data from the beacons in hand, the NSA and the Israelis set to work developing the bug itself, an enormously complex computer worm. It became a large operation, one that involved far more than just programmers well stocked with Diet Cokes. The bug had to be tested, and to test it they needed the P-1 centrifuges. Fortunately, the US government possessed a few—thanks to the "Mad Dog of the Middle East."

When Muammar Qaddafi gave up his nuclear weapons program in late 2003, he turned over everything A. Q. Khan had sold him—which investigators at the IAEA believe was similar to the package he had sold to the Iranians. (The Libyan treasure trove included a not-quite-complete Chinese bomb design that dated to the 1960s, and was clearly transferred to Pakistan years ago.) Since the IAEA didn't know where to store sensitive nuclear equipment, the centrifuges ended up at the heavily guarded Oak Ridge National Laboratory in Tennessee. They were still inside long, wooden boxes—some stamped KHAN RESEARCH LABORATORIES. Qaddafi's nuclear team had looked at the prototypes and the design plans that came with them and apparently given up. But Iranian engineers had been more diligent, and they set about building their own variant of the P-1.

Soon the military and intelligence officials overseeing Olympic Games managed to borrow a few centrifuges for what they delicately termed "destructive testing." Those first, small-scale tests were a success: only when Bush saw the remnants of a destroyed centrifuge was he convinced the program could work. Soon, from small factories around the country, the United States was secretly producing its own P-1s, perfect replicas of the centrifuges that the Iranians were using. The Siemens controllers were widely available on the open market; they are a common, fairly inexpensive piece of

hardware used in an incredible variety of manufacturing plants; no one would raise an eyebrow when front companies were sent out to buy them.

But there was concern that any large-scale test to run and destroy these outdated centrifuges would give away the project, so the work was spread out over several of the Energy Department's national laboratories, from Oak Ridge to the Argonne National Laboratory in Chicago to the Idaho National Laboratory, where—in one of those wonderful ironies of history—the US government has set up a center to help American companies defend themselves against cyberattacks.

"We had banks of these [centrifuges] we were building," one participant told me. Soon began the "destructive testing," an effort to see if the bug could do what it was intended to do: transmit a command that would lead large numbers of centrifuges to run out of control and ultimately self-destruct.

The tests grew more sophisticated; the bug was tried against mockups of the next generation of centrifuges the Iranians were expected to deploy, called IR-2s, and successor models, including some the Iranians still are struggling to construct. It was ready to be tested in Iran—once again inserted by embedding it on laptops and thumb drives headed into Natanz.

Once there, the worm sat, waiting and watching. It recorded what the "normal operation" of the plant looked like. This was critical, because there was a feature of the worm that would be familiar to moviegoers who watched the comedic remake of the thriller *Ocean's Eleven.* In one of the most memorable—and hilarious—scenes in the movie, a team of extraordinarily talented thieves lay the groundwork for their heist by tapping into the circuitry of the security cameras that monitor activity inside the vault that is supposed to hold the winnings from three of Las Vegas's biggest casinos. Then, as part of an elaborate con, they broadcast previously recorded footage onto

monitors in the casino control room. The casino's operators are deceived; meanwhile, the vault is cleaned out.

The worm did something very similar—and fooled the operators of Natanz just as George Clooney's character deceived a slimy casino operator. For weeks before the attack happened, the bug recorded the electronic signals indicating that the centrifuges were operating normally. Then it played those back just as the computer worm was taking control, spinning the centrifuges to enormous speeds, or slamming on their brakes. The plant operators were clueless. There were no warning lights, no alarm bells, no dials gyrating wildly. But anyone down in the plant would have felt, and heard, that the centrifuges were suddenly going haywire. First came a rumble, then an explosion.

"This may have been the most brilliant part of the code," one American official acknowledged. Later, word circulated through the IAEA that the Iranians had grown so distrustful of their own instruments that they assigned people to sit in the plant and radio back what they saw. "This really freaked them out," one official familiar with the operation of the plant old me.

For the longest time, the Iranians did not seem to understand that more than just bad luck, and bad parts, were causing the problem. "Even then, it took a while for them to figure out what exactly was happening." To keep them off balance, the participant said, "we kept changing the modalities of the attack," churning out new versions of the bug. The idea was not only to slow Iran's ability to produce enriched uranium; it was to mess with Iran's best scientific and military minds.

"The intent was that the failures should make them feel they were stupid, which is what happened," the participant in the attacks said. When a few centrifuges failed, the Iranians would close down whole "stands" that linked 164 machines, looking for possible sabotage in all of them. "They overreacted," one participant in the

American-Israeli attacks said. "And that delayed them even more." A few months later, Israeli and American officials began sharing reports of finger-pointing inside Iran's scientific infrastructure. "We soon discovered they fired people."

Later, imagery recovered by the nuclear inspectors from the monitoring cameras installed at Natanz—which is how the IAEA keeps track of what happens between visits—showed the results. There was some evidence of wreckage, but it was clear the Iranians had also carted away centrifuges that had previously appeared to be working well.

"Previous cyberattacks had effects limited to other computers," Michael D. Hayden, the former chief of the CIA, told me, declining to say what he knew about these attacks when he was in office. "This is the first attack of a major nature in which a cyberattack was used to effect physical destruction. And no matter what you think of the effects—and I think destroying a cascade of Iranian centrifuges is an unalloyed good—you can't help but describe it as an attack on critical infrastructure."

"Somebody has crossed the Rubicon," Hayden observed. "We've got a legion on the other side of the river now. I don't want to pretend it's the same effect, but in one sense at least, it's August 1945," the month that the world first saw capabilities of a new weapon, dropped over Hiroshima. That was a deliberate overstatement—this was a weapon of precise destruction, not mass destruction—but Hayden's point was an important one. In the hands of others, it could become a weapon of mass destruction.

BY THE TIME Barack Obama had settled into the presidency, Olympic Games was the best hope the United States and Israel had in slowing the Iranian nuclear program. Bush had launched a critical effort, Obama's team agreed. At the insistence of Defense Secretary Robert Gates, the program had been shifted over from military

command to the intelligence community. That meant that President Obama had to review and renew a set of presidential findings that would allow the United States to attack the nuclear infrastructure of a country with which we were not at war.

It was Obama's introduction to the new world in which he would soon be immersed. In the days before his inauguration, he had already been through the usual briefings every new president gets—the lesson about how to use the nuclear codes, carried in a briefcase, "the football" that would be near him at all times. General Cartwright, who conducted that briefing, has often told the story of Obama's reaction: after Cartwright talked him through the nuts and bolts of how to order the launch of nuclear weapons, Obama said he wasn't sure he would remember it all. Would Cartwright be able to come back in a few days, after the inaugural hubbub died down? Of course, the general said. A few days into his presidency, Obama passed word on to Gates: "You know that guy who scared the shit out of me? Can I talk to him again?"

But within a few weeks, a second team arrived, and the education of the president about cyberweapons began. Large foldout maps of the Natanz plant were spread across the Situation Room, as a series of officials went through the details of where the United States could implant technology to get at the centrifuges. Various options were described—from interfering with the plant's electrical supply to attacking the controllers—along with assessments of the preliminary results of the bug's first attacks on Natanz. Soon those diagrams of the Iranian enrichment process were showing up every few weeks in the Situation Room, marked to indicate where there were vulnerabilities. "Iran has been one of the president's highest priorities, and it's fair to say there wasn't a major strategic or tactical decision made without him," one White House official told me. Obama had choices to make about when and how to launch the next attacks. He listened and asked a few questions, but he was not as interested in the technological details as Bush had been, his briefers sensed.

What animated the new president were questions about the implications of this new weapon. What kind of collateral damage might occur? If a cyberattack focused on compromising the power grid that supplied Natanz, as the Bush administration had contemplated, might it trigger some other, unanticipated harm to civilians? "We didn't want to be cutting off the electricity to hospitals," one participant in the discussions with Obama said. What were the chances the Iranians would figure out the source of the attacks, and how might they respond? Obama thought it highly unlikely the Iranians would be able to respond in kind—the country's cyber capabilities appeared less than impressive—but they could certainly pull off "asymmetric attacks" on American troops, on Israel, on Saudi oil facilities. How well had the United States and its allies hardened their bases and oil facilities in case they became the natural target?

Obama also insisted, early on, that the bug had to be "unattributable," meaning he wanted the program to remain totally covert, for as long as possible. "He recognized there was a risk of attribution," one official said. "That's always a risk. But it's worth taking because of the need to effect the program."

In fact, for months before Obama took office, the Iranians appeared to have their suspicions. The NSA was increasingly successful at tuning in to the exchanges between Iranian scientists, engineers, and their superiors. "They were having a hard time understanding which of their problems were of their own making and which were not," one official said. Moreover, accounts of President Bush's approval of new ways to undermine the Iranian program, including attacks on its computer systems, appeared just as the Bush administration was packing up in January 2009. And at both the Pentagon and inside the intelligence agencies, some of the creators of the bug believed that it might be even more valuable if the source of the attacks became known, because the Iranians would get the message that Washington could pierce its systems repeatedly.

"The thinking was that the longer it could stay unattributable, the better," a participant in the discussions with Obama told me. "But we had to be ready to work in an environment where the Iranians knew exactly who was doing this to them, to make the point that we could come back and do it again."

As they settled in, many in the National Security Council grew uncomfortable simply extending Bush's covert program without a full review of its implications. Tom Donilon ordered a detailed review of all of Bush's old findings on Iran and the authorizations for covert action, with an eye toward reviewing and rewriting them so that Obama didn't run into a problem with a program that was simply on autopilot. (Most presidential findings are reviewed annually anyway, but this was a far more thorough scrub.) But up on the executive floor of the CIA, and deep in the bowels of the National Security Agency, the architects of Olympic Games feared that if the old findings were withdrawn, the activity would have to stop while Obama's team rewrote the others. In the intelligence world, "people started to go nuts," one official involved said, "because we'd have to pull everybody out and we'd erase the knowledge we had gained."

Eventually that problem was solved, and the Bush findings were simply amended. But over the course of 2009, more and more people inside the Obama White House were being "read into" the cyber program, even those not directly involved. As the reports from the latest iteration of the bug arrived, meetings were held to assess what kind of damage had been done, and the room got more and more crowded. The good news was that with each hit, the Iranians were losing more centrifuges, or spending so much time avoiding new problems that they could not focus on expanding their program as fast as they had hoped.

Then, in the early summer of 2010, trouble hit. Big trouble.

Several weeks before public reports appeared about a mysterious new computer worm, carried on USB keys and exploiting a hole in the Windows operating system, the creators of the bug realized that

random copies were floating around the globe. They were found disproportionately in Iran, Indonesia, and India. But how had it happened? Why was a computer worm that had been painstakingly designed to release itself only if detected by computer controllers connected to a specific array of centrifuges at Natanz suddenly zipping through the Internet like a newly released videogame?

The answer appeared to be one that Microsoft and every software manufacturer has discovered sooner or later: poorly tested new releases of software can generate all kinds of unanticipated results.

In this case, the problem lay in a torqued-up new version of the worm. In the spring of 2010, the White House, the NSA, and the Israelis had decided to swing for the fences. They had a specific, large array of centrifuges at Natanz in their sights—a critical array of nearly a thousand machines whose failure would be a huge setback for the Iranian project. A special variety of the worm was developed that would go into Natanz. The program was supposed to detect the presence of the centrifuge controllers and deploy itself. The Israelis had put the finishing touches on the ingenious program.

As American officials later reconstructed events, an Iranian scientist had plugged his laptop into the controllers at Natanz, and the worm hopped aboard. The bug had identified the network it was on—the centrifuge system—and began to do its work. But when the laptop was later unplugged from the secret network and reconnected to the Internet, the worm apparently did not recognize that its environment had changed. That's when things began to go haywire.

"The program began to think of the Internet as its little, private network," said one official who was briefed on what went wrong. It started propagating its code. Suddenly, the secret worm that the Americans and Israelis had invested millions of dollars and countless hours perfecting was showing up everywhere, where it could be picked apart.

"There is a lot of question about who was at fault," said one official. "But there is no question it was a fuck-up." The initial blame was put on the Israelis, who were the last ones to have their hands on that version of the code. But later analysis suggested that the Americans might have been equally at fault.

The release led to a series of panicked meetings. Was Olympic Games over? Or would the world be sufficiently confused about the origins of the worm that American deniability could be preserved?

Inside the Pentagon and the CIA, there were meetings about whether the United States would be accused of being among the first to use a cyberweapon against a sovereign state. Obama and Vice President Joe Biden called for briefings, and had to be persuaded that the virus would not hurt anything beyond its intended target. "The real damage was that we all had egg on our faces," said one official, "and now we were closer to the possibility that the Israelis would feel that this cyber experiment was over and they had to bomb."

Within weeks, as predicted, news stories started to appear, first in the technical press, then in mainstream newspapers. Soon, this worm had a name: "Stuxnet." (The name was an amalgam of some key words found in the software code, but they had no real meaning. The term "Stuxnet" had never been used by the United States or the Israelis.) Suddenly a worm no one had ever seen coming appeared on front pages around the world. Conspiracy theories abounded: It was the work of Russian criminals; of Chinese cyberspooks; of Israel, because of a number that seemed to refer to the date of the assassination of an Iranian-Jewish philanthropist who was killed in 1979. And of course, some thought it was so sophisticated it had to be the work of the United States.

Within days, the code was being picked apart by experts from Silicon Valley to Germany, where Ralph Langner, an independent computer security expert, began dissecting the bug with his staff and running it through the bank of Siemens computer controllers

he kept in his chalet-style offices. "It's like a playbook," he told me when I went to visit him just after Christmas 2010 in Hamburg. He described a worm that had what he called a "dual warhead." While it was widely spread, it kicked into effect only if it found the specific controllers that were connected to a configuration that fit the array of centrifuges at Natanz. "The attackers took great care to make sure that only their targets were hit," he said. "It was a marksman's job."

The very fact that Langner had a copy of the bug indicated that the marksman had missed a shot. Deciding they had little to lose, the Americans and Israelis issued another version of the code, this one with the error fixed. Then another one. The third time was a charm. In Natanz, 984 centrifuges came to a screeching halt.

IT DID NOT take long for the IAEA inspectors, who were clueless about the origins of the attack, to discover that about a fifth of Natanz's operating centrifuges had been taken offline since Stuxnet hit. It took months to get them working again. In the meantime, the Iranian Atomic Energy Organization announced that its engineers were trying to protect their facilities from the worm, even while denying it had done much damage. "The effect and damage of this spy worm in government systems is not serious," declared Reza Taghipour, a top official of Iran's Ministry of Communications and Information Technology.[4]

In Washington, a new debate began. Had the creators of this cyberattack on Iran erred by focusing too intently on a narrow set of Iranian vulnerabilities—those spinning centrifuges—instead of other areas? What else could this cyberweapon hit? And in the end, what was accomplished?

FOR ALL THE fears in the Situation Room that early summer day in 2010 when the president learned of the mistake that begot Stuxnet, there is no reason to believe America's cyber wars have ceased. Iran remains the number-one target. Some senior officials in the US government express dismay that we had not used this cyber capability, even in an earlier, primitive form, against North Korea's nuclear infrastructure once it began enriching uranium.

But the harder question to resolve is how successfully the bug prevented the Iranians from their goals. A senior American defense official estimated to me that it caused a year or two of delay, mostly because the Iranians shut down their facilities for fear that other attacks were on the way. Perhaps because the attack was the intelligence community's project, its estimate of success is more generous: its officials told the White House that Olympic Games delayed Iran's progress by two to three years. In fact, it's almost impossible to know the truth. But one fact is clear: Natanz was built to hold fifty thousand centrifuges. Today, after nearly a decade of continuous work, the Iranians have installed about a fifth of that number.

Still, a review of Iran's production records, released by the IAEA, suggests that by speeding up the centrifuges that were still working, Iran's output of enriched uranium did not decline. In short, Stuxnet was a setback, but not a crippling one.

Olympic Games put additional time on the clock, however. It gave Obama a chance to rally the allies to push for more effective sanctions, cut off oil revenues, and close down banking relationships. What it has not done, at least so far, is force the mullahs to give up their project. Olympic Games was not cost-free, however. The United States lost a bit of the moral high ground when it comes to warning the world of the dangers of cyberattacks. The next time the Chinese are confronted with evidence that they are launching cyberattacks against the US or its allies, Beijing is bound to offer up an easy one-liner: "So?

Explain how what we may be doing is different from what you did in Iran."

IN SEPTEMBER 2011, the Department of Homeland Security invited reporters for the first time to the cyber-emergency response center it built in Idaho Falls. Just on the edge of town, DHS installed a simulated chemical company and connected its equipment to computer controllers built by Honeywell, Siemens, and other major manufacturers. Then they set up a "red team"—a simulated competitor chemical company with the mock name of Barney Advanced Domestic Chemical, or BAD—to attack the system and try to bring it down.

It wasn't a fair fight, or a lengthy one. In cyberattacks, all the advantages lie with the attacker—the element of surprise, the ability to hit multiple weak spots at once, the mystery of where the attack is coming from. A team of "defenders" trying to protect the mock chemical company was quickly overwhelmed; when you walked downstairs, a small automated chemical factory appeared to be in chaos, with liquid spills occurring all the time, mixing machines shaking, black smoke pouring out for effect. The operators of the machinery were unable to shut any of it off, because the attackers had taken control of the electrical system too.

"We're connecting equipment that has never been connected before to this global network," Greg Schaffer, a DHS official, told us. "As we do, we have the potential for problems. That, indeed, is a space our adversaries are paying attention to. They are knocking on the doors of these systems. In some cases, there have been intrusions."

Of course, the Stuxnet virus was on the lips of each reporter, with everyone in Idaho Falls assuming that government officials knew more about it than they were saying. They probably didn't;

only later did I learn how closely held Olympic Games had been kept. But they knew enough to have the wisdom to declare their ignorance of Stuxnet's origins (and to demonstrate a remarkable lack of curiosity on the subject). It's not clear at all that they knew that a few miles away, behind high walls, the Idaho lab had been the place where the United States was testing out some of its P-1s in a classified effort to conduct exactly the kind of attack they had gathered us to warn against. The closest they would come to discussing Stuxnet was to comment on its importance as a wake-up call: it was a "game-changer," said Marty Edwards, who runs the control systems security program for DHS. Several years before, Edwards had invited Siemens to undergo a study of the vulnerability of its systems; a year later, those exact same vulnerabilities were exploited by the bug that the United States and Israel designed. Now, Edwards and others were fretting that elements of Stuxnet were being pulled apart by experts around the world, and that inevitably those elements would be used against the United States.

As Ralph Langner later said to me, "Now that Stuxnet's in the wild, you don't need to be a rocket scientist. You've got a blueprint of how to do it."

WHILE A SUCCESSION of computer worms were wreaking havoc in Natanz, Shahram Amiri, the Iranian scientist who had disappeared in Saudi Arabia, was settling into a new life in the southwest United States. He had taken on an entirely assumed identity—and he was miserable.

Even before Amiri defected through Saudi Arabia, the CIA had offered to attempt to bring his family with him, a senior intelligence officer told me. It was not possible; apparently Amiri's wife, from whom he was increasingly estranged, balked. So he had decided to

come alone. At first, he was so busy being debriefed and discovering life in the United States that the pain of separation was eased. But eventually the debriefings wound down and doubts and fears set in.

Amiri missed his young son desperately and over time could not resist the temptation to call home. He quickly discovered that the Iranian intelligence agencies, now aware that he had defected, were putting his family under huge pressure. By some accounts, they seized the family's passports so they could not join him. On one of Amiri's calls, Iranian intelligence officials answered and threatened to hurt his seven-year-old son. His only option, the Iranians told him, was to make a videotape claiming he had been kidnapped.[5]

By early April 2010, the pressure was just too great. So Amiri sat down in front of a webcam and repeated the story the Iranians had been pushing: "I was kidnapped last year in the holy city of Medina on June 3, in a joint operation by the terror and abduction units of the American CIA and Saudi Arabia's Istikhbarat," Amiri said. He described being drugged and tortured. Finally, he asked for help.[6]

Curiously, Iranian state television did not broadcast the video for two months. In the interim, Amiri had apparently felt pangs of guilt about bending to the Iranian authorities. So he told his American handlers about the webcast. It was hardly the first time a defector had reconsidered: Washington was full of stories of spies who returned to the cold, including the case of a Soviet defector who met his handlers in Georgetown, then ran out of a restaurant only to end up back in Moscow a few days later, to the CIA's huge embarrassment.

Eager not to be blindsided by the Amiri video, the CIA decided to fight YouTube with YouTube. Just hours after the Iranian broadcast, a well-shaven Amiri showed up on the Web telling a very different story. Sitting down in front of professional cameras in a well-furnished, warmly lit library, Amiri now contradicted most of what he had said in the earlier webcast.

In Amiri's revised story, he had come to the United States voluntarily to pursue a higher degree. "I am free here and I assure

everyone that I am safe," Amiri said. He never quite explained why his family remained at home, and watching the two videos back-to-back makes your head spin.

American officials later said the CIA had meant to get ahead of the Iranians and air their video first, but had screwed up the project.[7] As the propaganda war accelerated, Amiri's wife, Azar, told Iranian state television that the second video looked staged. "His deliberate method of speech showed that he was reading text; he wasn't speaking of himself, he was reading," she said. "How can a man with a child in the first grade . . . so easily say he is pursuing graduate study and will return when it is over?"[8]

Iranian state TV broadcast a third video three weeks later, with Amiri once again reverting to the story that he had been kidnapped. This time, he said, he had escaped from US custody and "could be rearrested at any time." He described his second video—the one in which he said he was pursuing his studies—as "a complete fabrication." Later, a senior American intelligence official told me that Amiri had spent weeks telling his handlers he had made a huge mistake defecting to the United States and just wanted to go home and be with his son. The Americans told him the stories of what had happened to Soviet defectors who returned home in the Cold War—only to be tortured or imprisoned. They explained what they thought happened to other Iranian scientists who had been detained on suspicion of revealing nuclear secrets. None of it registered. "He was just very emotional," the official said. "He kept saying, if I can only see my son's face for five minutes, I don't care if everything else you have warned me about comes true."

The rules of the resettlement program are clear: if a defector wants to return home, the United States has no legal basis to hold him. By July, Amiri had made his way back to the Washington area. One evening he hopped a cab and showed up at the Iranian interests section of the Pakistani embassy, a few hundred yards from the edge of the vice president's residence. He declared that he

wanted to return to Iran. When I called over to the embassy to ask if Amiri would agree to be interviewed before he left the country, the Pakistani who answered the phone hung up. Amiri did, however, give an interview to Iran's Press TV describing how he had been captured: he was drugged in Saudi Arabia, he said, and woke up on a military plane to the United States.

"During my stay there I was never free," Amiri said. "I was not allowed to use the Internet or any communication device, which is the first definition of freedom."[9]

On July 15, 2010, Amiri landed in Tehran. The Iranians created a heartwarming scene: He was greeted at the airport by his seven-year-old son and dozens of journalists and government officials, who laid a wreath of flowers around his neck. At a press conference, he claimed the United States had offered him millions to tell the press that he was a political refugee and knew the ins and outs of Iran's nuclear program. "I think that anyone in my position would not be ready to sacrifice their honor for material concerns," Amiri said.[10]

He staged an impressive piece of political theater. But even as Iran was rolling out the red carpet, there were clues that the hero's welcome would not last long. During a trip to Portugal, Iran's foreign minister, Manouchehr Mottaki, was asked whether Amiri could be regarded as a national hero. "We will see what has happened over these past two years, and afterwards we will see if he will be considered a hero," Mottaki said.[11] US officials also publicly countered Amiri's claims about having been tortured. "His safety depends on him sticking to that fairy tale about pressure and torture," one official said. "His challenge is to try to convince the Iranian security forces that he never cooperated with the United States."[12]

Amiri made one last appearance on Iranian television, giving an extensive interview on his ordeal. He maintained that he had no specific nuclear knowledge and had never even been inside the facilities at Qom or Natanz. (American officials think this state-

ment was accurate.) The Americans, he said, suffered from bad intelligence and had mistaken him for an expert on Iran's activities. "My familiarity with nuclear sites in Iran may even be less than that of an ordinary person," Amiri said, his face shiny with sweat.[13] He seemed short of breath and sounded nervous.

Within days, he disappeared. Isolated reports have emerged from sites run by the Iranian opposition reporting his arrest and torture on charges of revealing state secrets. American officials say they would be surprised if they ever see or hear from him again.

NOT ONLY WERE the CIA, the NSA, and the Mossad doing their best to undermine the nuclear program, but the VOA—the Voice of America—did its best to undercut the entire Khamenei regime.

No one actually thought they were up to it. America's own government-funded broadcaster still operates from the same fortress-like headquarters on the Washington Mall where it fought Cold War censorship. If you were to walk into the lobby, in fact, you would be forgiven for thinking that the era of Mao and Stalin never ended. The hallways are long, gray, and uninviting. Pictures on the walls recall the glory days of VOA, when the oppressed masses in the Soviet Union, Eastern Europe, and Communist corners of Asia surreptitiously gathered around their radios, figuring that if they had to choose between local propaganda and Washington's view of the world, they would prefer Washington's. Long after the Berlin Wall had fallen and parents had to explain to their children what Communists were, VOA programming could be sleep-inducing, with a lot of emphasis on what farming life was like in small-town Iowa. And while VOA has modernized many of its studios, and has gotten pretty savvy about the Web, there are still pieces of broadcasting equipment hanging around that look like they are awaiting shipment to the Smithsonian a few blocks down the

street. It's worth remembering that when VOA was in its heyday, subtly offering up a vision of life in the capitalist West, the founders of Twitter and Facebook were yet to be born.

But in recent times, perhaps VOA's biggest shortcoming was that its broadcasts were humorless and utterly lacking in irony. Despite the earnest efforts of many directors who were determined to yank it into the twenty-first century, the programming always sounded more Edward R. Murrow than Jon Stewart.

That was until two Iranian exiles, Kambiz Hosseini and Saman Arbabi, came up with the insight that there were no better subjects for rapier-like parody than two somewhat bumbling rivals: Iran's supreme leader and his nemesis, President Mahmoud Ahmadinejad.

Hosseini and Arbabi knew their audience: 70 percent of Iranians are American-obsessed youth, many of whom know their way around the Comedy Central website. Hosseini and Arbabi realized that the one attack the Iranian leadership would never be ready for is a Persian-language show that uses satire and audience engagement to cement the image of Iran's ossified leadership as a bunch of argumentative fools who would rather enrich uranium than enrich the economy.

And so, from a group of cubicles on Constitution Avenue, with a budget of well under a million dollars, they developed a satellite television show that arguably does more to undermine the Iranian leadership than billions of dollars in antimissile defenses, sanctions, and computer viruses ever could. Thus was born *Parazit* (which translates as "static")—the Persian answer to *The Daily Show*.

It would be wonderful to imagine that this stroke of brilliance arose from some ingenious thinking in the White House Situation Room or a conference over at the State Department. No such luck. It was entirely the brainchild of Hosseini and Arbabi, who do not exactly fit the VOA mold. Today, tens of thousands of people, sometimes hundreds of thousands, go to extraordinary lengths to watch the show—fine-tuning their satellite dishes and searching

for Internet connections that the Iranian authorities have not yet found and disabled.

"We know it's been successful," David Ensor, the head of Voice of America, said to me late in 2011, "because the Iranians put such enormous effort into trying to block it."

No wonder. The running theme of the shows is the endless war between the supreme leader and his president, which plays out each week in Tehran in the form of petty insults, political humiliations, and the periodic arrest of Ahmadinejad loyalists. The intricacies of this palace intrigue, which Iranians know about in fanatical detail, provide the kind of grist for *Parazit* that the battles between the traditional Republican Party and the Tea Party provide for *The Daily Show*. It helps that Hosseini and Arbabi have an intimate understanding of the Iranian psyche—and of the fact that nothing is more dangerous to the supreme leader than the sense that his country is laughing at him.

"With Iran we have almost nothing else," said Ramin Asgard, who was the director of the Persian News Network, VOA's Persian-language channel. It was actually like the old Cold War days, when there was so little two-way communication between the United States and the target country of its broadcasts that the broadcasts themselves are the primary way to send a message. In the case of *Parazit,* the message is clear: your nation is being run by a bunch of crazies who can't figure out what's in their own best interests.

Kambiz Hosseini came to the United States only twelve years ago, from Rasht, in northwest Iran, a city known for the intellectual bent of its residents. As a teenager during the Iran-Iraq War, he starred in an early-morning children's radio program, *Flower Buds of the Islamic Revolution,* in which he acted out skits imbued with the Shi'a Islamic ideal of martyrdom. "They made me say things that I don't believe right now," Hosseini told me during a visit to VOA's studios.[14] But

he loved the atmosphere and the freedom it hinted at. In college he worked under a New Wave filmmaker, studied experimental theater, and became a fan of Woody Allen and Harold Pinter. When Hosseini arrived in the United States in 2000, one of his plays was being performed in Tehran's most famous theater. But he pumped gas for his first job in the United States. "I didn't know a word of English," he recalled, which disqualified him for many things except a full-time job at VOA's Persian service, so he joined in 2005.

He became the host of *Shabahang,* a cultural program that was about as dull as a VOA broadcast can be. "I wasn't in charge, and the people who were in charge, they didn't know what they were doing," he complained.

Saman Arbabi, in his late thirties, is taller than Hosseini by several inches and gives off the disheveled, laidback air of a guy who doesn't really want to show up for a day job. He has a seemingly endless supply of graphic T-shirts that he wears untucked. And during each *Parazit* episode, he stands off-camera; his job is to introduce wacky video clips with pithy one-liners. But his main role is as executive producer, in which he focuses on the emotional impact of the show—down to selecting the soundtrack of Iranian and American rock music. He knows them both well, as he lived in Iran until 1985 and had what you might call a nontraditional upbringing: his father was an atheist in a country dedicated to perpetual Islamic revolution, and his political views leaned toward those of Iran's Communist Party. When Saman was twelve, he moved to Rockville, Maryland, the heart of Washington suburbia. He describes himself as a "horrible student" and a class clown; as a young man, he worked the grill at a local Hooters to pay his tuition. His goofy antics won the attention of a producer for a local television affiliate, who gave him an internship, and he was quickly hooked. In 2004, he got a call from VOA, which was expanding its Persian service, and soon he traveled to Afghanistan and the Middle East.

Hosseini and Arbabi knew each other socially, and they started griping at a bar one night that the broadcast had nothing that would speak to Iran's young people in their own cynical, sarcastic language. "We were bored and tired," Hosseini recalled. So the two typed up their fledgling idea for a show and presented it to Alex Belida, the director of the Persian News Network at the time. Astoundingly, he did not say no. "He knew this was a breath of fresh air. He knew at the very least this could entertain kids in Iran," Arbabi said.

Belida suggested they begin with ten-minute segments, which Arbabi described as "very fast-paced mini-documentaries." The first episodes aired in late spring of 2009, just after Obama took office and several months before the Iranian presidential elections.

The show gained more and more popularity when the rigged 2009 presidential elections in Iran led to street protests. Then, suddenly, a largely apolitical entertainment show became intensely political, as its hosts readily admit. "To do anything else at the time would have been ridiculous for the Iranian audience," he emphasized. "We found our niche and said, 'This is why we're here, to cover this.' We went a hundred and twenty percent political with Iranian news."

With so much else blacked out, viewers inside the country turned to Hosseini and Arbabi, who beamed back to them images of the protestors, bloodied and wearing green, marching to rock and rap music while being beaten by police. "People picked us up from that point on and we had to just follow them," Hosseini said. "They couldn't identify with anyone else in the media at the time." VOA eventually figured out what it had and gave the two their own half-hour, weekly prime-time slot.

The brilliance of the show is that it makes its point by avoiding most direct politics and instead focuses on the ridiculous, like the time Ahmadinejad boasted of Iran's launch of a satellite and declared that "God willing, we will send a second, bigger satellite

into space that will be there for one year. Once we send a satellite more than one thousand kilometers, we can, with that same missile, reach thirty-five thousand kilometers. There, the direction is all downhill."

The camera cuts to Hosseini, who leans forward in his seat, incredulous and eyebrows arched. "It's downhill? In space? You go a thousand kilometers . . . and then it's downhill? Really, thank you, you're making us all proud."

Then, there was the moment that the commander of the much-feared Islamic Revolutionary Guard Corps, which Hillary Clinton had declared was responsible for Iran's slide into military dictatorship, offered to send the corps to the Gulf of Mexico to help clean up the BP oil spill.

"The IRGC is going to go to the Gulf of Mexico to clean up the oil?" Hosseini asked. "Do you even know what goes on in the Gulf of Mexico? Mexican music, everyone's naked, they're all dancing, love and good times, tequila.

"Mr. Qasemi," Hosseini continued, as mariachi music played, "if you come here to the Gulf of Mexico, you'll put the principles of the revolution in danger. You'll have to work with your eyes shut, and you can't clean up anything with eyes shut."

Even Shahram Amiri, the Iranian nuclear spy who returned to an uncertain fate, was a source of parody. While the CIA played down the embarrassment of losing a major asset who had provided information about Iran's secret programs, a routine on *Parazit*—funded by the same government that brought Amiri here—portrayed him as "The Man with Three Thousand Faces." Their own Amiri character was a portly, mustachioed man huddled over his laptop, making videotapes while obviously being coached by an off-camera character.

"This chubbiness that you see," their Amiri character says, explaining his weight gain when he hit American shores, was an occupational hazard. "I was in the past thin," he said, "but during imprisonment and torture I became like this."

The most daring segments take on the supreme leader himself, always dangerous business. They recently played one tape of Khamenei declaring, "According to principles, I am not going to interfere in government affairs and decisions. Except in the case that"—and here Khamenei's eyebrows rise and he points his index finger—"I feel the best interests of the people are being harmed."

"Yes," Hosseini cut in. "We have laws, *except in the case that* Mr. Khamenei feels differently."[15]

Inevitably, Hosseini says, there were threats to his family back in Iran. His relatives, he said, were told, "Tell him you can do whatever you want and we won't touch your family if you stay away from Khamenei." With evident bravado, Hosseini said his response was to make fun of Khamenei for the full half hour on the next show.

It is difficult to measure the effect of satire, just as it is tricky to assess lasting damage done by computer worms. But as Arbabi said, "What we've done is something the US government has not been able to do in thirty-two years. We have these governments who don't talk to each other." At least now, there is a way of communicating, even if it involves putting in the knife and twisting it a bit.

MEIR DAGAN IS built like a fireplug. Short and bald, he rarely smiles, and he speaks in the sharp, declarative sentences of a warrior who has survived life in a tough neighborhood and appreciates the need for occasional ruthlessness. In conversation, he is quite emphatic about how the world works and views those who question the certainties of the Middle East with a slight cock of his head and an expression that seems to say, "You must have grown up someplace else." He also speaks with the discretion of a man who grew up protecting the deepest secrets of the Mossad, which he ran until he was forced into retirement in 2011, after a long, festering argument with the two men at the head of the government: Prime Minister Benjamin Netanyahu and Defense Minister Ehud Barak. Both

made clear to Dagan that they intended to solve the Iran nuclear problem, permanently, on their watch. And both saw Dagan as an obstacle.

If Dagan is bitter about anything these days, it is about the way he was treated at the end of his term—when Netanyahu and Barak refused to reappoint him as the head of the Mossad. He wasn't alone: they also eased out the heads of three other security services, all of whom had roughly agreed with Dagan's assessment that Israel still had sufficient time to deal with the Iran problem. On his way out the door, Dagan had told the Knesset, Israel's parliament, that Iran's "technological difficulties"—a phrase that meant to encompass the cyberattacks—could delay the country's ability to build a bomb until 2015. Netanyahu and Barak believed this assessment, while consistent with the view of American intelligence agencies, was not only optimistic—it was dangerous. The world would not gather to confront a threat it thought might be distant.

By firing Dagan, Netanyahu created a permanent, highly credible opposition figure, who until recently had daily access to the same intelligence that the prime minister himself did. And so after a few months of nursing his wounds, Dagan began publicly voicing his view: not only was Iran a few years from a real weapon, he said, but a direct, obvious "attack on Iran's nuclear reactors would be foolish."

It was not that Dagan was willing to let Iran get a weapon; far from it. He was just certain, as were the Americans, that a military attack was the surest way to guarantee that, in the fullness of time, Iran would become a nuclear weapons state. Iran would emerge from an attack more unified than ever, and more determined to build a bomb. And that debate—within Israel and between Israel and the Obama administration—became the animating argument of 2011 and 2012, pushing aside all other issues in the relationship, including peace with the Palestinians.

In that argument, Dagan has extraordinary standing. Over the

course of forty years, he had shown he was more than willing to kill, sabotage, and attack on Israel's behalf. Talk to him for ten minutes, and you hear the voice of an unabashed hawk.

His mentor in the Israeli establishment had been Ariel Sharon, who appointed him to head the Mossad in the summer of 2002. Sharon and Dagan had known each other for decades, and in the early 1970s, Sharon, then a top commander in the Israeli Defense Force, assigned Dagan the grisly task of assassinating key Palestinian Liberation Organization militia in the Gaza. He took to the job with considerable enthusiasm. Sharon's assessment of Dagan quickly became legend: "Dagan's specialty is separating an Arab from his head."[16]

In 2007, it was Dagan who showed up in Stephen Hadley's West Wing office and threw down on his coffee table a portfolio of pictures of a nuclear reactor under construction in Syria, based on a North Korean design. You must destroy this facility, Dagan said, or my government will. President Bush declined to bomb it, after his aides feared that risking a war in yet another Islamic nation would put Bush in a category no American president wants to be in. (Vice President Dick Cheney, by his own account, was the only one in the Bush administration who argued in favor of the United States destroying the Syrian reactor, partly as a warning to Iran that it could be next.) In September 2007, the Israelis sent bombers over Syria that did the job. Today, that incident is used by advocates of an airstrike on Natanz and Qom as an example of a successful preemptive strike, though against a far closer, far easier target.

It was Dagan who ordered what became known, derisively, as the "Dubai Job," the killing, in a hotel room in Dubai, of a Hamas leader named Mahmoud al-Mabhouh. While the operation succeeded, it was done with an astounding absence of good tradecraft by young Mossad officers who were caught on camera entering and exiting the hotel where the assassination took place. That led to an unraveling of how they operated, including forging passports from countries

allied with Israel. Diplomatic demarches and much embarrassment followed.

The mismanaged killing in Dubai was a rare blemish on Dagan's career, and it helped create a pretext for the decision not to extend his tenure. Dagan believes he and Israel's other intelligence chiefs were replaced because they had pushed back so hard against Netanyahu's determination to terminate the Iranian program with an overt strike.

"He's convinced that Netanyahu wanted to surround himself with his own team, loyalists who will not push back if the order goes out to launch a full attack on the nuclear sites," one of President Obama's senior advisers told me in the fall of 2011. "And we think that's probably the right analysis, and it's changed the dynamic inside the Israeli government."[17]

But when Dagan kept up his criticism of the military-attack option, he found himself in an open war with Netanyahu's government. His diplomatic passport was pulled. Barak, the defense minister, shot back on Israeli radio that Dagan was harming "Israel's ability to deter" the Iranians.[18]

There was considerable irony to that line of attack. Just a year before, no one inside the Israeli government spent more of their days thinking about new ways to sabotage the Iranian program than Dagan himself. Many of the early assassinations of Iranian scientists occurred on his watch, and it reminded some Israelis of Dagan's earlier days running an elite assassination squad against Hamas leaders. When the first discussions of cyberattacks on Iran took place, Dagan periodically sat in on the secure video conferences between Jerusalem and Washington, planning out the operations. He was not involved day-to-day, several officials told me, but checked in regularly to see that the cyberattacks were on track.

The cyberattacks' success did not dazzle the rest of the Israeli establishment. Netanyahu and Barak argued to the Americans that they were kidding themselves if they thought computer worms and

sanctions would do any more than delay the inevitable. At some point, Iran would make enough progress that its capability to build a bomb would be unstoppable.

For a country like Israel, dedicated to never allowing a Holocaust to happen again, letting that situation fester was simply unacceptable. Netanyahu and Barak often pointed to the attack on the Osirak reactor in Iraq in 1981 and the attack on the Syrian reactor in 2007 as models for the kind of preemptive strike that Israel was poised to conduct in Iran. In fact, when Netanyahu came to Washington in March 2012 with talk of war in the air, he echoed the words of Menachem Begin, Israel's prime minister during the Iraq raid thirty years before. "We chose this moment, now, not later, because later may be too late," Begin had said in the days after the 1981 raid. "And if we stood by idly, two, three years, at the most four years, Saddam Hussein would have produced his three, four, five bombs."

Dagan had no patience for such talk. He shot back that Iran was a different case. Saddam had put all his eggs into one, lightly guarded basket; so had the Syrians. Iran had learned from those mistakes. Iraq's key target was aboveground; Iran's are deep below. Iraq's nuclear infrastructure was pretty well understood; much of Iran's remains a mystery.

What's more, Dagan appeared convinced by the American argument that Iran had suspended much of its nuclear weapons research in 2003, and has only resumed it sporadically. "I haven't yet seen any decision to cross the line and obtain a nuclear weapons capability," he said, breaking with the official Israeli view. "I see an approach to shorten the distance" to a bomb.

Dagan argued that exploiting Iran's many internal divisions would be the wisest strategy. Iran's fractured religious groups don't all accept the supreme leader, and he is not considered a particularly strong religious authority. The clerics in Qom—the side of town that worried about the future of Shi'ism, not the future of centrifuges—

were particularly critical of him. There were other divisions between moderates in the urban centers and more rabid conservatives in the rural areas. The military was divided too, between ordinary forces and the Islamic Revolutionary Guard Corps. And within the Revolutionary Guard, many were worried that sanctions were cutting into their most profitable businesses.

A smart policy would focus on worsening these rifts, Dagan contended, urging Israeli and American officials alike to "go directly against the regime itself. There is real division there." Bombing would have the opposite effect, unifying the country behind the mullahs, giving Iran the excuse to throw out inspectors and take the program deep underground.

"What Dagan believes is that the key element to building a bomb is the knowledge, and you can't bomb knowledge," one American who dealt with him often said. "In a few years, we'd be dealing with this all over again." To Netanyahu and Barak, this was woolly-headed thinking: regime change in Iran would be nice—but nothing Israel can bank on. Its timing is unpredictable and a successor government may be no less committed to a nuclear weapons option. Going after the capability, not the government, would be the only real guarantee, they said.

But Dagan's arguments, even after he was forced out, blew the long-simmering debate out of Israel's cabinet rooms and into the open. In the fractious, always overheated world of Israeli politics, many joined in, including former chiefs of staff of the Israeli Defense Force and the former leaders of Shin Bet (the internal security service) and other intelligence agencies. Israeli journalists told me that the Mossad itself, heavily invested in both Dagan and the sabotage efforts it had executed, was actively leaking word that many of its own top officers were worried about the huge risks of blowback from an overt strike.

"We are in a strange world," one senior Israeli official said to me, "where the defense minister and to a lesser degree the prime

minister are focused intently on the military option, and the intelligence services and the military, with some exceptions, are deeply doubtful." Partly that was because of turf battles: the Mossad believes its campaign of sabotage and assassinations has successfully set back the Iranians for years, and with a few more explosions like the one that wiped out the giant missile development base, they could buy more time.

But in a debate like this, the Iranians also get a vote. As Israel argued, Iran focused more and more on uranium enrichment—and bringing to life that huge underground installation at Qom, under rock so deep the Israelis could not strike it.

Both were potential game-changers, and by the spring of 2012, Washington and Jerusalem talked ceaselessly of impending war.