A Declaration of Cyber-War

Last summer, the world’s top software-security experts were panicked by the discovery of a drone-like computer virus, radically different from and far more sophisticated than any they’d seen. The race was on to figure out its payload, its purpose, and who was behind it. As the world now knows, the Stuxnet worm appears to have attacked Iran’s nuclear program. And, as Michael Joseph Gross reports, while its source remains something of a mystery, Stuxnet is the new face of 21st-century warfare: invisible, anonymous, and devastating.

By Michael Joseph Gross
Photograph by Jonas Fredwall Karlsson

A self-replicating computer virus, called a worm, was making its way through thousands of computers around the world, searching for small gray plastic boxes called programmable-logic controllers—tiny computers about the size of a pack of crayons, which regulate the machinery in factories, power plants, and construction and engineering projects. These controllers, or P.L.C.’s, perform the critical scut work of modern life. They open and shut valves in water pipes, speed and slow the spinning of uranium centrifuges, mete out the dollop of cream in each Oreo cookie, and time the change of traffic lights from red to green.

Although controllers are ubiquitous, knowledge of them is so rare that many top government officials did not even know they existed until that week in July. Several major Western powers initially feared the worm might...
O
ne month before that midnight summons—on June 17—Sergey Ulasen, the head of the Anti-Virus Kernel department of VirusBlokAda, a small information-technology security company in Minsk, Belarus, sat in his office reading an e-mail report: a client’s computer in Iran just would not stop rebooting. Ulasen got a copy of the virus that was causing the problem and passed it along to a colleague, Oleg Kupreev, who put it into a “debugger”—a software program that examines the code of other programs, including viruses. The men realized that the virus was infecting Microsoft’s Windows operating systems using a vulnerability that had never been detected before. A vulnerability that has not been detected before, and that a program’s creator does not know exists, is called a “zero day.” In the world of computer security, a Windows zero-day vulnerability signals that the author is a pro, and discovering one is a big event. Such flaws can be exploited for a variety of nefarious purposes, and they can sell on the black market for as much as $100,000.

The virus discovered by Ulasen was especially exotic, because it had a previously unknown way of spreading. Stick a flash drive with the virus into a laptop and it enters the machine surreptitiously, uploading two files: a rootkit dropper (which lets the virus do whatever it wants on the computer—as one hacker explains, “‘Root’ means you’re God”) and an injector for a payload of malicious code that was so heavily encrypted as to be, to Ulasen, inscrutable. The most unsettling thing about the virus was that its components hid themselves as soon as they got into the host. To do this, the virus used a digital signature, an encrypted string of bits that legitimate software programs carry to show that they come in peace. Digital signatures are like passports for software: proof of identity for programs crossing the border between one machine and the next. Viruses sometimes use forged digital signatures to get access to computers, like teenagers using fake IDs to get into bars. Security consultants have for several years expected malware writers to make the leap from forged signatures to genuine, stolen ones. This was the first time it was known to have actually happened, and it was a doozy of a job. With a signature somehow obtained from Realtek, one of the most trusted names in the business, the new virus Ulasen was looking at might as well have been carrying a cop’s badge.

What was this thing after that its creators would go to such extravagant lengths? Ulasen couldn’t figure that part out—what the payload was for. What he did understand was the basic injection system—how the virus propagated itself—which alone demanded an alert. Ulasen and Kupreev wrote up their findings, and on July 5, through a colleague in Germany, they sent a warning to the Microsoft Security Response Center, in Redmond, Washington. Microsoft first acknowledged the vulnerability the next day. Ulasen also wrote to Realtek, in Taiwan, to let them know about the stolen digital signature. Finally, on July 12, Ulasen posted a report on the malware to a security message board. Within 48 hours, Frank Boldewin, an independent security analyst in Muenster, Germany, had decrypted almost all of the virus’s payload and discovered what the target was: P.L.C.’s. Boldewin posted his findings to the same security message board, triggering the all-points bulletin among Western governments.
The next day, July 15, a tech reporter named Brian Krebs broke the news of the virus on his blog. The day after that, Microsoft, having analyzed the malware with the help of outside researchers, issued the first of several defenses against the virus. At this point it had been detected in only a few sites in Europe and the U.S. The largest number of infections by far—more than 15,000, and growing fast—was found in Asia, primarily in India, Indonesia, and, significantly, Iran.

In the process of being publicly revealed, the virus was given a name, using an anagram of letters found in two parts of its code. “Stuxnet” sounded like something out of William Gibson or Frank Herbert—it seethed with dystopian menace. Madison Avenue could hardly have picked a name more likely to ensure that the threat got attention and to take the image of a virus viral.

Yet someone, apparently, was trying to help Stuxnet dodge the bullet of publicity. On July 14, just as news of its existence was starting to spread, Stuxnet’s operators gave it a new self-defense mechanism. Although Stuxnet’s digital signature from Realtek had by now been revoked, a new version of Stuxnet appeared with a new digital signature from a different company, JMicron—just in time to help the worm continue to avoid detection, despite the next day’s media onslaught. The following week, after computer-security analysts detected this new version, the second signature, too, was revoked. Stuxnet did not attempt to present a third signature. The virus would continue to replicate, though its presence became easier to detect.

On July 15, the day Stuxnet’s existence became widely known, the Web sites of two of the world’s top mailing lists for newsletters on industrial-control-systems security fell victim to distributed-denial-of-service attacks—the oldest, crudest style of cyber-sabotage there is. One of the first known acts of cyber-warfare was a DDoS attack on Estonia, in 2007, when the whole country’s Internet access was massively disrupted. The source of such attacks can never be identified with absolute certainty, but the overwhelming suspicion is that the culprit, in that instance, was Russia. It is not known who instigated the DDoS attacks on the industrial-control-systems-security Web sites. Though one of the sites managed to weather the attack, the other was overloaded with requests for service from a botnet that knocked out its mail server, interrupting a main line of communication for power plants and factories wanting information on the new threat.

The secret of Stuxnet’s existence may have been blown, but clearly someone—someone whose timing was either spectacularly lucky or remarkably well informed—was sparing no effort to fight back.

omens of doomsday

The volcanoes of Kamchatka were calling to Eugene Kaspersky. In the first week of July, the 45-year-old C.E.O. and co-founder of Kaspersky Lab, the world’s fourth-largest computer-security company, had been in his Moscow office, counting the minutes until his Siberian vacation would start, when one of his engineers, who had just received a call about Stuxnet from Microsoft, came rushing in, barely coherent: “Eugene, you don’t believe, something very frightening, frightening, frightening bad.”

After VirusBlokAda found Stuxnet, and Microsoft announced its existence, Kaspersky Lab began researching the virus. Kaspersky shared its findings with Microsoft, and the two undertook an unusual collaboration to analyze the code. Symantec, ESET, and F-Secure also published extensive analyses of Stuxnet, and Symantec later joined Microsoft’s formal collaboration with Kaspersky to study the worm.

Kaspersky is a 1987 graduate of the Soviet Institute of Cryptography, Telecommunications and Computer Science, which had been set up as a joint project of the K.G.B. and the Russian Ministry of Defense. He has beetling gray eyebrows and a flair for the dramatic. He drives a Ferrari, sponsors a Formula 1 racing team, and likes Jackie Chan movies so much that he hired Chan as a company spokesman. It would be an exaggeration to say that Stuxnet thrilled him, but he and many of his colleagues had been waiting for something like this to happen for years. Computer security, like many of the fixing professions, thrives on unacknowledged miserabilism. In omens of doomsday, its practitioners see dollar signs. As one of Kaspersky’s top competitors told me, “In this business, fear is my friend.”
To help lead his Stuxnet team, Kaspersky chose Roel Schouwenberg, a bright-eyed, ponytailed Dutch anti-virus researcher who, at 26, has known Kaspersky for almost a decade. (When he was in high school, Schouwenberg took it upon himself to troll the Web for viruses and, for fun, e-mail daily reports on them to the C.E.O. he had read about online.) Analysts at Kaspersky and Symantec quickly found that Stuxnet exploited not a single zero-day flaw but in fact four of them, which was unprecedented—one of the great technical blockbusters in malware history.

As the zero days piled up, Kaspersky says, he suspected that a government had written Stuxnet, because it would be so difficult and time-consuming for an outsider to find all these flaws without access to the Windows source code. Then Kaspersky lowers his voice, chuckles, and says, “We are coming to the very dangerous zone. The next step, if we are speaking in this way, if we are discussing this in this way, the next step is that there were a call from Washington to Seattle to help with the source code.”

To Schouwenberg and many others, Stuxnet appears to be the product of a more sophisticated and expensive development process than any other piece of malware that has become publicly known. A Symantec strategist estimated that as many as 30 different people helped write it. Programmers’ coding styles are as distinctive as writers’ prose styles. One expert estimated that the worm’s development took at least six months. Once Stuxnet was released into the wild, other technicians would have maintained the command-and-control servers in Denmark and Malaysia to which Stuxnet phoned home to report its current locations and seek updates.

Most curious, there were two major variants of the worm. The earliest versions of it, which appear to have been released in the summer of 2009, were extremely sophisticated in some ways but fairly primitive in others, compared with the newer version, which seems to have first circulated in March 2010. A third variant, containing minor improvements, appeared in April. In Schouwenberg’s view, this may mean that the authors thought Stuxnet wasn’t moving fast enough, or had not hit its target, so they created a more aggressive delivery mechanism. The authors, he thinks, weighed the risk of discovery against the risk of a mission failure and chose the former.

There seemed no end to the odd surprises that Stuxnet had to offer. In a July 15 posting, Alexander Gostev, who wrote Kaspersky Lab’s blog on the worm, mysteriously quoted from a botanical entry in Wikipedia: “Myrtus (myrtle) is a genus of one or two species of flowering plants in the family Myrtaceae.”

“Why the sudden foray into botany?,” Gostev asked. His answer: “Because the rootkit driver code contains the following string: b:\myrtus\src\objfre_w2k_x86 \i386\guava.pdb.” Gostev went on to raise the specter of a “Project ‘Myrtus’” and added portentously: “To be continued?” Although Gostev never returned to his musings on Stuxnet’s botanical allusion, he had planted a seed that would very quickly sprout.

At the end of July, just before Eugene Kaspersky came home from the volcanoes, Schouwenberg started trying to persuade a writer from The New York Times to cover Stuxnet. Without specific information on the source or the target, though, the topic was a nonstarter. Then, on September 16, an industrial-control-systems-security expert in Hamburg made a sensational blog posting about Stuxnet, whose deployment he would soon dub “operation myrtus.” And he was pretty sure he knew what the myrtle reference signified. The man had never been quoted in a newspaper before, but he was about to shift the global conversation about Stuxnet in a radically new direction.

self-directed stealth drone

“I’m I crazy, or am I a genius?” The question would not leave Ralph Langner alone. He was having trouble sleeping. Sometimes he thought the C.I.A. was watching him. Langner, a voluble man of 52, is built like a whippet, with short hair neatly parted to the side. His Hamburg-based company is a big name in the small world of industrial-control-systems security, and counts some of Germany’s largest automotive and chemical corporations among its clients. Langner had been reverse engineering the payload of Stuxnet throughout August, and he was the first analyst to announce that it contained two components that he called “warheads.” Langner had come to believe that Stuxnet was aimed at Iran’s nuclear program. Iran has been suspected of trying to build a nuclear bomb for several years, and in 2003 it failed to...
disclose details regarding uranium-enrichment centrifuges to inspectors from the International Atomic Energy Agency. Western governments have been trying to stop Iran’s nuclear program ever since, using diplomatic pressure, trade embargoes, and covert operations.

Stuxnet had initially grabbed the tech world’s attention as a hack of the Windows operating system—a virus that exploited an unknown vulnerability. This was like learning that someone had found his way into your house, and figuring out how they got inside. Next, Frank Boldewin had discovered what valuables the intruder was after—programmable-logic controllers. Specifically, the target was P.L.C.’s made by the German engineering conglomerate Siemens. Finally, Langner figured out the rudiments of what Stuxnet’s payload did—that is, how the intruder went about his work. When Stuxnet moves into a computer, it attempts to spread to every machine on that computer’s network and to find out whether any are running Siemens software. If the answer is no, Stuxnet becomes a useless, inert feature on the network. If the answer is yes, the worm checks to see whether the machine is connected to a P.L.C. or waits until it is. Then it fingerprints the P.L.C. and the physical components connected to the controller, looking for a particular kind of machinery. If Stuxnet finds the piece of machinery it is looking for, it checks to see if that component is operating under certain conditions. If it is, Stuxnet injects its own rogue code into the controller, to change the way the machinery works. And even as it sabotages its target system, it fools the machine’s digital safety system into reading as if everything were normal.

Industrial-control systems have been sabotaged before. But never have they been remotely programmed to be physically altered without someone’s fingers on a keyboard somewhere, pulling the virtual trigger. Stuxnet is like a self-directed stealth drone: the first known virus that, released into the wild, can seek out a specific target, sabotage it, and hide both its existence and its effects until after the damage is done. This is revolutionary. Langner’s technical analysis of the payload would elicit widespread admiration from his peers. Yet he also found himself inexorably drawn to speculation about the source of the malware, leading him to build a detailed theory about who had created it and where it was aimed.

Near the start of September, Langner Googled “Myrtus” and “Hebrew” and saw a reference to the book of Esther, a biblical story in which Jews foil a Persian plot against them. He then Googled “Iran” and “nuclear,” looking for signs of trouble, and discovered that the Bushehr power plant had been experiencing mysterious construction delays. (Although Bushehr is only a power plant, its nuclear reactor could produce plutonium in low-enriched uranium fuel that could be re-purposed for weapons.) Next, Langner sent an e-mail about Stuxnet to his friend Joe Weiss, who organizes the top industrial-control-systems cyber-security conference in the U.S. (and wrote the standard book on the topic, Protecting Industrial Control Systems from Electronic Threats). Langner would later post that e-mail to his blog: “Ask your friends in the government and in the intelligence community what they know about the reasons why Bushehr didn’t go operational last month. BTW, did somebody from Israel register to attend the conference?:”) Eventually, Langner decided to just put it out there. He would post his theory that Stuxnet was the first literal cyber-weapon, and that it had been aimed by Israel at Bushehr, and see what happened.

Plenty happened. The Christian Science Monitor published a report on Langner’s theory on September 21. The next day, a German newspaper published an article by another German computer expert, Frank Rieger, claiming that, in fact, the cyber-weapon had been aimed not at Bushehr but at Iran’s Natanz uranium-enrichment facility. The Iran speculation pinged across the Web. Two days later, Riva Richmond posted a version of Langner’s theory on the Times’s technology blog, Gadgetwise. The Times’s David E. Sanger then took the ball and ran with it, suggesting that Stuxnet may have been part of a covert U.S. intelligence operation to sabotage Iran’s nuclear program that had started under President George W. Bush and had been accelerated after Barack Obama took office. One Iranian-government official reportedly admitted that the worm had been found in government systems, but another official claimed that the damage was “not serious.” Then the Iranian government announced that it had arrested “nuclear spies,” possibly in connection with the Stuxnet episode, according to the Times. Rumors swirled online that the accused spies had been executed.
"If I did not have the background that I had, I don’t think I would have had the guts to say what I said about Stuxnet," Langner says now, finishing his second glass of wine during lunch at a Viennese restaurant in Hamburg. Langner studied psychology and artificial intelligence at the Free University of Berlin. He fell into control systems by accident and found that he loved the fiendishly painstaking work. Every control system is like a bespoke suit made from one-of-a-kind custom fabric—tailored precisely for the conditions of that industrial installation and no other. In a profession whose members have a reputation for being unable to wear matching socks, Langner is a bona fide dandy. “My preference is for Dolce & Gabbana shoes,” he says. “Did you notice, yesterday I wore ostrich?” Langner loves the attention that his theories have gotten. He is waiting, he says, for “an American chick,” preferably a blonde, and preferably from California, to notice his blog and ask him out.

Last fall Langner and I spent two days together in Hamburg, including some time in the office where he and his employees demonstrated Stuxnet’s attack method on computers and Siemens controllers they had infected with the malware. Langner’s office is comfortable but spare. Industrial-control security is not very lucrative, mostly because industry does not do much to guard the safety of its processes. A minority of industries in a minority of countries are forced to do so by regulation. The U.S. regulates systems security only for the commercial nuclear-power industry and, to a much lesser extent, the chemical industry. This laissez-faire arrangement has created vulnerabilities that Stuxnet laid bare.

Because there has as yet been no calamitous, headline-grabbing cyber-attack on critical civilian infrastructure, many corporations see Langner and his ilk as boys crying wolf. Langner, who talks with his hands, arms, and elbows, finds such criticism upsetting and confusing. He frequently stretches to full wingspan and then wiggles all 10 fingers, as if playing a piano, to emphasize a point, and many of his points amount to bewilderment that owners of critical infrastructure can be so stupid as not to see the threats he sees. Still, he is not without hope. From the moment he released his Iran story on the Web, he says, one of his fondest wishes has been that “someday the world would say, Thank you, Ralph. You were right.”

On November 12, Stuxnet analysts caught a huge break. After receiving a tip from a Dutch computer expert, a researcher at Symantec, in California, which had by now become the most prominent analyst of the virus, announced that the company had identified the specific target of one of Stuxnet’s two warheads. This warhead, as it turned out, was aimed at frequency-converter drives, which can be used to control the speed of spinning centrifuges. Specifically, when Stuxnet finds a particular configuration of frequency-converter drives made by the Iranian company Fararo Paya and the Finnish company Vacon, the worm runs rogue code to alter the drives’ speed. If the drives were connected to centrifuges, this could damage or destroy the machines. The warhead also runs another set of code, concealing the change that it has made.

For Frank Rieger, who had been the first to argue that Stuxnet was aimed at the centrifuges in Natanz, this news came as vindication. A few weeks later, in Berlin, the morning after a fresh snowfall, Rieger stomped into the Chaos Computer Club (C.C.C.) hacker space, a giant rec room on Marienstrasse full of fake surveillance cameras, beat-up leather sofas, and lots of softly whirring fans cooling lots of computer processors. Rieger’s dark-blue-gray jumpsuit was caked with ice from his morning commute, which he makes on a large tricycle regardless of the weather. Beefy and taciturn, Rieger serves as spokesman for the C.C.C., the second-largest human-rights technology group in the world (after the Electronic Frontier Foundation). The group calls itself “a galactic community of life forms, independent of age, sex, race or societal orientation, which strives across borders for freedom of information.”

Unlike Langner, who enjoys publicity, Rieger seems leery of attention. He tries not to talk about sensitive topics via cell phone or e-mail, because, he says, “I do not want to become a person of interest.” In fact, he is already a person of interest: it was a U.S. government official who urged me to visit Rieger, saying that his research “is the closest thing to the true picture of Stuxnet that has been made public yet.”
During the summer, Rieger had traveled to six European countries to meet with members of each nation’s Stuxnet-analysis group. He spoke with high-level intelligence sources in three of those countries. He told me that all three have provisionally concluded that Stuxnet was a joint operation of the U.S. and Israel.

Based on these conversations, Rieger came to believe that Stuxnet was deployed by a U.S. intelligence organization, not a military unit, because intelligence operations are more deniable and their activities are seldom regarded as overt acts of war—even if the resulting damage has war-like effects. Rieger believes Stuxnet was spread by the Israeli intelligence agency Mossad. He points out that the assassination of one Iranian nuclear scientist and the attempted killing of another in Tehran on November 29 employed techniques similar to those used in other attacks by Mossad. (Mossad could not be reached for comment.)

Stuxnet, Rieger suggests, may be a new expression of a long-standing American tradition of sabotaging enemy technology. During the Reagan administration, France gave the U.S. a cache of secret Russian documents known as the Farewell Dossier, which included a shopping list of Western computer software and hardware that the Soviets wanted. Based on this intelligence, the U.S. and Canada conspired to put faulty controllers in Russian hands, in due course causing an explosion on the trans-Siberian gas pipeline so large that it could be seen from space. In their book, *Fallout*, Doug Frantz and Catherine Collins describe covert joint operations involving the C.I.A., Mossad, and M.I.6 to sabotage critical components for Iran’s nuclear program, and Frantz speculates that the failure of those operations may have driven the intelligence agencies to make the leap to remote cyber-sabotage with Stuxnet.

Rieger came away from his investigation preoccupied with the many ways in which Stuxnet blurs old boundaries: “The interesting question, since it is in this gray area between military and intelligence and statecraft, is: Who controls these kinds of weapons politically? Who’s in charge of making sure they are used only against legitimate enemies?” With the arrival of weapons such as Stuxnet, Rieger says, clear lines of conflict between nations will be “grayed out into a fog of possibilities and options.”

In spite of Stuxnet’s many muddling effects, it also offers a clear answer to one of cyber-war’s most difficult problems. Academics and software developers have long wondered how cyber-attacks could be weaponized but remain side-effect-free. If you aim a cyber-weapon at a power station, how do you avoid taking out a hospital at the same time? “Stuxnet is a really good example of how to do that,” Rieger says, “how to make sure that you actually only run on the system that you’re targeting.” To Rieger, Stuxnet’s success on this point “shows that the effort put into its development has been on not just a technical level but a strategic level too, thinking through: How should the proper cyber-weapon be constructed?”

Stuxnet’s code telegraphs the inherent caution of its makers in yet another way: it has “fail-safe” features to limit its propagation. The USB-spreading code, for instance, limits the number of devices that each infected device can itself infect. (The limit is three, enough to create a moderate chain reaction, but not so many that its effects would rage out of control.) Most dramatically, on June 24, 2012, the worm will self-destruct altogether: erase itself from every infected machine and simply disappear. Analysts disagree on whether some of the code’s fail-safes actually work.

Richard Clarke, the former chief of counter-terrorism under Presidents Clinton and Bush, believes the fail-safes are an important clue to the malware’s source—they point to a Western government: “If a government were going to do something like this, a responsible government, then it would have to go through a bureaucracy, a clearance process,” he says. “Somewhere along the line, lawyers would say, ‘We have to prevent collateral damage,’ and the programmers would go back and add features that normally you don’t see in the hacks. And there are several of them in Stuxnet. It just says lawyers all over it.”

Rieger’s hypothesis—that Natanz was the worm’s target—is now almost universally accepted as the explanation of Stuxnet’s purpose. Even Ralph Langner, the original Bushehr proponent, has come around to supporting it. The matter of attribution remains dicey, however, especially concerning the question of what role Israel may have played in the operation. Since last fall, those who believe
Israel was involved have pointed to apparent clues in the injector’s code, such as “myrtus.”

A further possible clue emerged in late December, when Felix Lindner, a Berlin security expert who goes by the nom de guerre “FX,” announced that all manually written functions in Stuxnet’s payload bear the time stamp “24 September 2007”—which happens to be the day Iranian president Mahmoud Ahmadinejad spoke at Columbia University, in New York, and questioned whether the Holocaust had in fact occurred. Many cyber-warfare and intelligence experts, such as Sandro Gaycken, of the Free University of Berlin, say such signs are so obvious that they could well be “false flags,” planted to mislead investigators and complicate attribution.

There is a marked difference in design style between Stuxnet’s injector and its payload. Tom Parker, a Washington, D.C.- based security researcher, argues from this fact that two nations were involved in the worm’s creation, implying that a major Western power, such as the U.S., may have developed the sleek warheads and that another nation, such as Israel, was responsible for the injector program.

Once the two elements were married, the entire package might then have been delivered to someone with access to Natanz (or to a related installation). Wittingly or not, this Patient Zero began the infection process, perhaps by plugging a USB flash drive into a critical network. The virus probably spread with the help of foreign contractors and engineers, whose computers were infected during visits to Iranian installations.

Those skeptical of a U.S.-Israel scenario find it implausible because, as one former intelligence officer explained, the level of trust between the two countries’ intelligence and military establishments is not high. Other former C.I.A. officers, including Reuel Marc Gerecht, now director of the Middle East Initiative at the Project for the New American Century, are more open to the possibility of an Israeli connection. Another former C.I.A. official believes that “the non-extraterritoriality” of Stuxnet would encourage the agency to engage in a joint operation. “You’re not putting a human being in harm’s way. Someone’s not personally carrying in something that could explode, spread disease, or emit radiation. It’s a totally harmless digital item.”

Indeed, it’s possible that more than one country was involved in Stuxnet’s deployment. Jordan is the object of much speculation. Majid Shahriari, the nuclear physicist who was killed in Tehran in November, was involved in a project called “Synchrotron-light for Experimental Science and Applications in the Middle East” (SESAME), which aims to build an international scientific-research center in Jordan. U.S. intelligence has long had trouble making contacts among Iranian scientists, according to Gerecht, and SESAME offered a possible opportunity, on friendly turf. “I wouldn’t be surprised,” he says, “if that were the primary, perhaps the only, harvesting ground for the individuals who put out the virus.” Gerecht notes that French, Israeli, and Jordanian intelligence have all monitored Iranian involvement in SESAME. Any of these countries could have helped facilitate Stuxnet’s deployment.

In January, when longtime Mossad chief Meir Dagan retired, more evidence of Israel’s involvement seemed to appear. Dagan said that the Iranian nuclear-weapons program had run into technical difficulties and been set back by several years, thanks in part to “measures that have been deployed against them”—a remark that some interpreted as a veiled reference to Stuxnet. (Citing the effectiveness of economic sanctions, Secretary of State Hillary Clinton endorsed this “setback” view.) The next week, on January 16, The New York Times reported that Israel had performed crucial tests on Stuxnet at a uranium-centrifuge test bed—which may have been a mirror site of the mechanical system at Natanz—constructed at the secretive Dimona weapons complex in the Negev Desert. Though the headline was stirring—ISRAEL TESTS CALLED CRUCIAL IN IRAN NUCLEAR SETBACK—the evidence was shaky.

Dimona does have a collection of centrifuges, but it is not known whether they include P-1s, which were peddled on the black market throughout the Middle East and Asia by Pakistani scientist A. Q. Khan and are among those used at Natanz. The Times story cited an anonymous nuclear-intelligence expert who said that Dimona tested Stuxnet on P-1-style centrifuges. And in asserting that “Israeli intelligence had asked retired senior Dimona personnel to help” with an operation concerning Iran, the story cited Avner Cohen, an expert on Israel’s weapons program, and the author of The Worst-Kept Secret:
Israel’s Bargain with the Bomb. But Cohen, when pressed, admitted to me that his own source for that information was secondhand.

Such connections do not necessarily implicate Israel in Stuxnet’s development—and the article’s better-documented evidence, though relegated to the background, actually concerned America’s involvement. The United States, too, has a cache of P-1s, and U.S. intelligence has advocated studying the machines’ vulnerabilities at least since 2004. The Times also made an argument that originated with Ralph Langner—that Siemens and the Idaho National Laboratory collaborated in 2008 on a study of some of the very same vulnerabilities in Siemens’s S7 controllers that would be exploited by Stuxnet. The Times wrote that I.N.L. refused to comment on whether it had shared information on those vulnerabilities with American intelligence. In a statement to Vanity Fair, a lab spokesman wrote, “Idaho National Laboratory was not involved in the creation of the STUXNET worm. In fact, our focus is to protect and defend control systems and critical infrastructures from cyber threats like STUXNET and we are well recognized for these efforts. We value the relationships that we have formed within the control systems industry and in no way would risk these partnerships by divulging confidential information.”

At Siemens headquarters, in Nuremberg, when I asked a technical specialist with firsthand knowledge of the company’s controller research with I.N.L. whether he or anyone else at Siemens had been involved in any way in the creation, testing, or deployment of Stuxnet, he responded, staring down into his lap, “You mean in the first place?,” and then, making eye contact not with me but with the company publicist, who was also in the room, answered, “No, to my best knowledge.”

Ralph Langner was the Times story’s only named source for technical information about Stuxnet, and one person who was interviewed for it told me that “John Markoff said that everything that was published [about the impact on Natanz] was based on Langner’s research. That’s troubling, because Ralph doesn’t know anything about centrifuges.” (Markoff, one of the story’s authors, says that he consulted multiple sources, and Langner admits, “I’m not a centrifuge expert,” but says that he regularly speaks with such experts.) Langner’s feelings about Iran sometimes color his explanations of Stuxnet to the press. In one e-mail exchange with me, he wrote, “An infection with Stuxnet doesn’t render the controller useless, [the controller] just needs to be reprogrammed and the problem is gone. I know I suggested a little bit different in my interview with the Jerusalem Post, but that was just one of my small efforts to make the situation even worse for Tehran.”

Gary Sick, a former member of the National Security Council who was the chief White House aide for Iran during the revolution and hostage crisis, was struck by the Times story’s timing. On January 20, just four days after the story was published, diplomatic negotiations on the Iranian nuclear program were scheduled to resume, this time in Istanbul. With President Obama under pressure to do more to curb Iran’s nuclear program, the Times story probably had a number of politically desirable effects, as Sick observes: “It takes the pressure off the U.S., takes some of the pressure off Israel, gives Meir Dagan a chance to pat himself on the back, makes the Israelis feel more confident of their connection with the U.S., and it gives the Americans more maneuvering room in the negotiations”—by expanding the margin of plausible deniability of U.S. involvement in Stuxnet. “What’s not to like?”

Cloak-and-dagger posturing about Stuxnet continues to swirl. According to the Israeli newspaper Haaretz, guests at a retirement party for Israel Defense Forces chief of staff Lieutenant General Gabi Ashkenazi watched a video tribute to his career highlights—which included a reference to Stuxnet.

Yet there is vanishingly little doubt that the United States played a role in creating the worm. Some of the evidence for this is lying in plain sight: a consistent pattern of coincidences ties Stuxnet’s evolutionary stages to milestones in the development of Iran’s nuclear program. At each of these points, which often led to heightened tensions between the U.S. and Iran, Stuxnet upped its game.

There is some consensus that the earliest samples of Stuxnet date to June 2009, the point of maximum instability of the government of President Ahmadinejad, when the streets of
Iran were filled with protesters against his election. The next month, WikiLeaks posted a note stating that an anonymous source had reported that there had been a nuclear accident at Natanz in early July. On July 16, the director of Iran’s nuclear program resigned. Official figures from the International Atomic Energy Agency (I.A.E.A.) later confirmed that a large number of centrifuges at Natanz had ceased to function around this time.

After U.N. inspectors visited a new uranium-enrichment plant being constructed near the Iranian holy city of Qom, tensions between the U.S. and Iran built steadily. In January 2010, Iran effectively rejected an I.A.E.A. proposal that would have required that most of its uranium enrichment take place abroad. The following week, the first sample of Stuxnet bearing a stolen digital signature appeared.

In February, the I.A.E.A. reported for the first time that Iran was actively seeking to produce nuclear weapons. The following month, Stuxnet added a new propagation mechanism: the ability to spread seamlessly and invisibly via USB sticks.

In April, Iran announced that it would begin construction of another uranium-enrichment plant. That month, the third variant of Stuxnet appeared. The United Nations, the European Union, and the United States all imposed new sanctions on Iran in June and July. At this same time, Stuxnet-infection numbers ballooned. And only in September, when saber rattling over Iran’s nuclear program peaked—reportedly, Israeli government leaders had come to believe that Iran would have the bomb by March 2011—did Stuxnet’s purported attack on Iran begin to be made public.

These coincidences suggest that Stuxnet’s evolution—and the public disclosure of its existence and alleged purpose—was deliberately paced and may have been coordinated with diplomatic and economic pressures to slow the progress of Iran’s nuclear program. Such measured tactical responses add to the sense that Stuxnet’s operators were circumspect about their sabotage, in ways that seem more characteristic of the U.S. than of Israel. As of this writing, I.N.L.’s statement to Vanity Fair is the first and only definitive statement by any U.S. government body either admitting or denying involvement in Stuxnet. When directly asked whether Stuxnet was part of a covert U.S. operation to sabotage Iran’s nuclear program, a C.I.A. spokesman declined to comment. A National Security Agency representative wrote via e-mail, “I don’t have any information to provide.” A U.S. Cyber Command official wrote, “U.S. Cyber Command has nothing further to add.”

Serious questions about Stuxnet’s genesis and effects remain. Not least is the question of what damage Stuxnet may actually have done to Natanz. Ahmadinejad, for what it’s worth, has claimed that Iran’s centrifuges fell victim to cyber-attack. The physicist David Albright, president of the Institute for Science and International Security (ISIS), has studied the possible impact on Natanz and found evidence of only a temporary slowdown. He says, “It appears on the surface that if they were attacked they have recovered and are moving on.” Yet based on a tip from Ralph Langner, combined with analysis by Symantec, ISIS asserted that the code of Stuxnet’s second warhead is hunting for an installation identical to a specific kind of centrifuge cascade at Natanz. Albright co-authored a report that called this “perhaps the strongest evidence” that Stuxnet is aimed at the facility. The same study posits that the worm did some “relatively limited damage” to Natanz. As a result, Albright is concerned that Iran “will feel they’ve been attacked and they can do something in return if they want to.”

Albright worries, too, that the deployment of tactics such as Stuxnet is being done without effective oversight: “The intelligence committees on the Hill don’t provide real accountability.”

The cyber-world where Stuxnet lives is so murky, so hard to know the truth about, that some experts still question certain elements of the public story. From the beginning, many have found it odd that, of all the security companies in the world, an obscure Belarusian firm should be the one to find this threat—and odder still that the serial rebooting that gave Stuxnet away has been reported nowhere else, as far as most of the worm’s top analysts have heard. Such facts moved one former C.I.A. official to suggest that perhaps Stuxnet was not actually discovered—but dropped. Maybe its limited impact on Natanz indicates that it was not fully successful as a cyber-operation. After being detected by Iran,
it may have been retooled by the country as “psyops”—psychological operations—against the West. Robert Baer, the former C.I.A. officer and author of *The Devil We Know: Dealing with the New Iranian Superpower*, says, “The moment Iran caught Stuxnet, they could easily have put out misinformation”—to the effect that their nuclear program had been set back several years—“simply to alleviate meetings in Western capitals. So that everyone will say, ‘All right, Stuxnet worked.’ ”

Regardless of how well it worked, there is no question that Stuxnet is something new under the sun. At the very least, it is a blueprint for a new way of attacking industrial-control systems. In the end, the most important thing now publicly known about Stuxnet is that Stuxnet is now publicly known. That knowledge is, on the simplest level, a warning: America’s own critical infrastructure is a sitting target for attacks like this. That aside, if Stuxnet really did attack Iran’s nuclear program, it could be called the first unattributable act of war. The implications of that concept are confounding. Because cyber-weapons pose an almost unsolvable problem of sourcing—who pulled the trigger?—war could evolve into something more and more like terror. Cyber-conflict makes military action more like a never-ending game of uncle, where the fingers of weaker nations are perpetually bent back. The wars would often be secret, waged by members of anonymous, elite brain trusts, none of whom would ever have to look an enemy in the eye. For people whose lives are connected to the targets, the results could be as catastrophic as a bombing raid, but would be even more disorienting. People would suffer, but would never be certain whom to blame.

Stuxnet is the Hiroshima of cyber-war. That is its true significance, and all the speculation about its target and its source should not blind us to that larger reality. We have crossed a threshold, and there is no turning back.