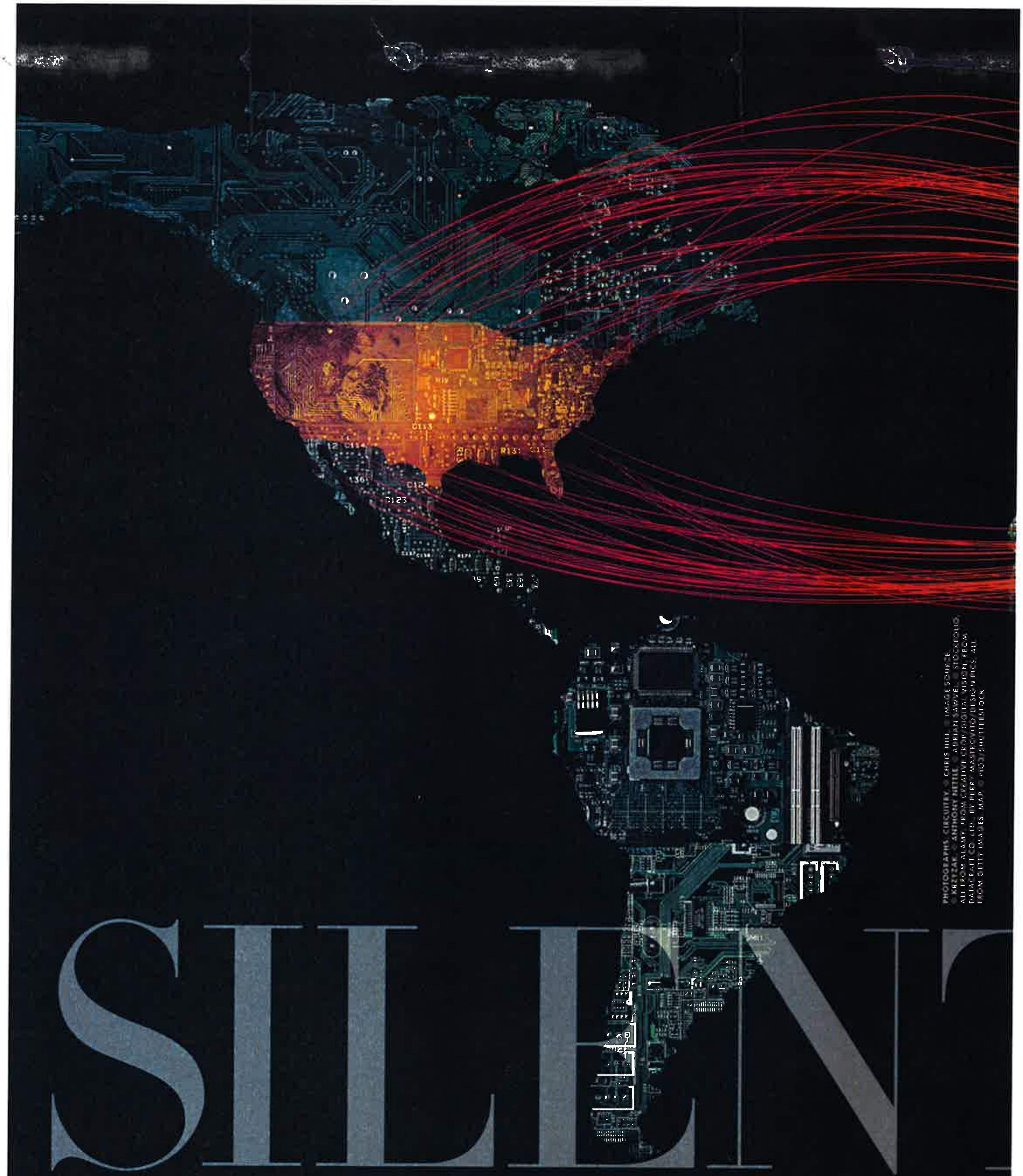


SILENT

On the hidden battlefields of history's first known cyber-war, the casualties are
seriously damaged, likely in retaliation for several major attacks on Iran. Washington and
enmeshing such high-tech giants as Microsoft, Google, and Apple. With the help of
the outbreak of the conflict, its escalation, and its startling paradox: that

PHOTOGRAPHS: CIRCUITRY, © CHRIS HILL, © IMAGE SOURCE, © KRZYZAK, © ANTHONY NETTLE, © ADRIAN SAWVEL, © STOCKFOLIO, ALL FROM ALAMY; FROM CREATIVE CROP/DIGITAL VISION; FROM DATACRAFT CO. LTD., BY PIERY MASTROVITO/DESIGN PICS, ALL FROM GETTY IMAGES. MAP, © PIXOJ/SHUTTERSTOCK.

SILICON VOLLEYS
There's no shooting—just clicking. The cyber-conflict between the United States (and its allies) and Iran (and its allies) is changing the definition of warfare.

T WAR

piling up. In the U.S., many banks have been hit, and the telecommunications industry
Tehran are ramping up their cyber-arsenals, built on a black-market digital arms bazaar,
highly placed government and private-sector sources, MICHAEL JOSEPH GROSS describes
America's bid to stop nuclear proliferation may have unleashed a greater threat

PHOTO ILLUSTRATION BY CHRIS MUELLER

I. Battlespace

Their eyeballs felt it first. A wall of 104-degree air hit the cyber-security analysts as they descended from the jets that had fetched them, on a few hours' notice, from Europe and the United States. They were in Dhahran, in eastern Saudi Arabia, a small, isolated city that is the headquarters of the world's largest oil company, Saudi ARAMCO. The group included representatives of Oracle, IBM, CrowdStrike, Red Hat, McAfee, Microsoft, and several smaller private firms—a SWAT dream team for the virtual realm. They came to investigate a computer-network attack that had occurred on August 15, 2012, on the eve of a Muslim holy day called Lailat al Qadr, "the Night of Power." Technically the attack was crude, but its geopolitical implications would soon become alarming.

The data on three-quarters of the machines on the main computer network of Saudi ARAMCO had been destroyed. Hackers who identified themselves as Islamic and called themselves the Cutting Sword of Justice executed a full wipe of the hard drives of 30,000 ARAMCO personal computers. For good measure, as a kind of calling card, the hackers lit up the screen of each machine they wiped with a single image, of an American flag on fire.

A few technical details of the attack eventually emerged into the press. Aboard the U.S.S. *Intrepid,* in New York Harbor, Defense Secretary Leon Panetta told a group of C.E.O.'s that the ARAMCO hack was "probably the most destructive attack that the private sector has seen to date." Technical experts conceded the attack's effectiveness but scorned its primitive technique. "It wrote over memory five, six times," one hacker told me. "O.K., it works, but it's not *sophisticated.*" Even so, many current and former government officials took account of the brute force on display and shuddered to think what might have happened if the target had been different: the Port of Los Angeles, say, or the Social Security Administration, or O'Hare International Airport. *Holy shit,* one former national-security official recalls thinking—*pick any network you want, and they could do this to it. Just wipe it clean.*

In the immediate aftermath of the attack, as forensic analysts began work in Dhahran, U.S. officials half a world away gathered in the White House Situation Room, where heads of agencies speculated about who had attacked ARAMCO and why, and what the attackers might do next. Cutting Sword claimed that it acted in revenge for the Saudi government's support of "crimes and atrocities" in countries such as Bahrain and Syria. But officials gathered at the White House could not help wondering if the attack was payback from Iran, using America's Saudi ally as a proxy, for the ongoing program of cyber-warfare waged by the U.S. and Israel, and probably other Western governments, against the Iranian nuclear program.

When the history of cyber-warfare comes to be written, its first sentence may go something like this: "Israel gave the United States an ultimatum." For a number of years, intelligence reports intermittently indicated that Iran was getting closer to building a nuclear bomb, which the Israeli leadership views as an existential threat. In 2004, Israel gave Washington a wish list of weapons and other capabilities it wanted to acquire. The list—for various kinds of hardware but also for items such as aerial transmission codes, so that Israeli jets could overfly Iraq without having to worry about being shot down by U.S. warplanes—left little doubt that Israel was planning a military attack to stop Iran's nuclear progress. President George W. Bush regarded such action as unacceptable, while acknowledging that diplomacy and economic sanctions had failed to change Iran's mind.

Intelligence and defense officials offered him a possible third way—a program of cyber-operations, mounted with the help of Israel and perhaps other allies, that would attack Iran's nuclear program surreptitiously and at the very least buy some time. As with the drone program, the Obama administration inherited this plan, embraced it, and has followed through in a major way. Significant cyber-operations have been launched against Iran, and the Iranians have certainly noticed. It may be that these operations will eventually change minds in Tehran. But the ARAMCO attack suggests that, for the moment, the target may be more interested in shooting back, and with weapons of a similar kind.

Cyberspace is now a battlespace. But it's a battlespace you cannot see, and whose engagements are rarely deduced or described publicly until long after the fact, like events in distant galaxies. Knowledge of cyber-warfare is intensely restricted: almost all information about these events becomes classified as soon as it is discovered. The commanding generals of the war have little to say. Michael Hayden, who was director of the C.I.A. when some of the U.S. cyber-attacks on Iran reportedly occurred, declined an interview request with a one-line e-mail: "Don't know what I would have to say beyond what I read in the papers." But with the help of highly placed hackers in the private sector, and of current and former officials in the military and intelligence establishments and the White House, it is possible to describe the outbreak of the world's first known cyber-war and some of the key battles fought so far.

ON EACH COMPUTER THE HACKERS WIPED, THEY LIT UP THE SCREEN WITH THE IMAGE OF AN AMERICAN FLAG ON FIRE.

II. Flame, Mahdi, Gauss

"I needed to come up with something cool for self-promotion at conferences," Wes Brown recalls. The year was 2005, and Brown, a hacker who is deaf and has cerebral palsy, started a business called Ephemeral Security with a colleague named Scott Dunlop. Banks and other corporations hired Ephemeral to hack their networks and steal information, then tell them how to keep bad guys from doing the same thing. So Brown and Dunlop spent a lot of time dreaming up ingenious break-ins. Sometimes they used those ideas to boost their street cred and advertise their business by making presentations at elite hacker conferences—elaborate festivals of one-upmanship involving some of the greatest technical minds in the world.

At a Dunkin' Donuts coffee shop in Maine, Brown and Dunlop started brainstorming, and what they produced was a tool for attacking networks and gathering information in penetration tests—which also amounted to a revolutionary model for espionage. By July of that year, the two men completed writing a program called Mosquito. Not only did Mosquito hide the fact that it was stealing information, but its spy methods could be updated, switched out, and re-programmed remotely through an encrypted connection back to a command-and-control server—"the equivalent of in-flight drone repair," Brown explains. In 2005 the unveiling of Mosquito was one of the most popular presentations at the prestigious hacker conference known as Def Con, in Las Vegas.

Many U.S. military and intelligence officials attend Def Con and have been doing so for years. As early as the 1990s, the U.S. government was openly discussing cyber-war. Reportedly, in 2003, during the second Gulf War, the Pentagon proposed freezing Saddam Hussein's bank accounts, but the Treasury secretary, John W. Snow, vetoed the cyber-strike, arguing that it would set a dangerous precedent that could result in similar attacks on the U.S. and de-stabilize the world economy. (To this day, the Treasury Department participates in decisions concerning offensive cyber-warfare operations that could have an impact on U.S. financial institutions or the broader economy.) After 9/11, when counterterrorism efforts and intelligence became increasingly reliant on cyber-operations, the pressure to militarize those capabilities, and to keep them secret, increased. As Iran seemed to move closer to building a nuclear weapon, the pressure increased even more.

As Wes Brown recalls, none of the government types in the audience said a word to him after his Mosquito presentation at Def Con. "None that I could identify as government types, at least," he adds, with a chuckle. But about two years later, probably in 2007, malware now known as Flame appeared in Europe and eventually spread to thousands of machines in the Middle East, mostly in Iran. Like Mosquito, Flame included modules that could, through an encrypted connection to a command-and-control server, be updated, switched out, and re-programmed remotely—just like in-flight drone repair. The Flame software offered a very full bag of tricks. One module secretly turned on the victim's microphone and recorded everything it could hear. Another collected architectural plans and design schematics, looking for the inner workings of industrial installations. Still other Flame modules took screenshots of victims' computers; logged keyboard activity, including passwords; recorded Skype conversations; and forced infected computers to connect via Bluetooth to any nearby Bluetooth-enabled devices, such as cell phones, and then vacuumed up their data as well.

During that same period, a virus that would be named Duqu—which targeted fewer than 50 machines, mostly in Iran and Sudan—began collecting information about the computer systems controlling industrial machinery, and to diagram the commercial relationships of various Iranian organizations. Duqu, like many other significant pieces of malware, was named for a feature of the code, in this case derived from the names the malware gave to files it created. In time, researchers found that Duqu bore several resemblances to an even more virulent cyber-attack.

As early as 2007, the first versions of a computer worm, designed not for espionage but for the physical sabotage of machinery, began to infect computers in several countries but primarily in Iran. As reported in these pages ("A Declaration of Cyber-War," April 2011), it was one of the most resilient, sophisticated, and noxious pieces of malware ever seen. The following year, after the worm got loose on the Internet, analysis by private experts swiftly produced a detailed conjecture regarding its source, aims, and target. Named Stuxnet, the worm appeared to have come from the U.S. or Israel (or both), and it seemed to have destroyed uranium-enrichment centrifuges at Iran's nuclear facility in Natanz. If the suppositions about Stuxnet are correct, then it was the first known cyber-weapon to cause significant physical damage to its target. Once released into the wild, Stuxnet performed a complex mission of seeking out and destroying its target. Jason Healey, a former White House official who now runs the Cyber Statecraft Initiative for the Atlantic Council, argues that Stuxnet was "the first autonomous weapon with an algorithm, not a human hand, pulling the trigger."

For the U.S., Stuxnet was both a victory and a defeat. The operation displayed a chillingly effective capability, but the fact that Stuxnet escaped and became public was a problem. Last June, David E. Sanger confirmed and expanded on the basic elements of the Stuxnet conjecture in a *New York Times* story, the week before publication of his book *Confront and Conceal.* The White House refused to confirm or deny Sanger's account but condemned its disclosure of classified information, and the F.B.I. and Justice Department opened a criminal investigation of the leak, which is still ongoing. Sanger, for his part, said that when he reviewed his story with Obama-administration officials, they did not ask him to keep silent. Accord-

CONSTRUCTION BY STEPHEN DOYLE

ing to a former White House official, in the aftermath of the Stuxnet revelations "there must have been a U.S.-government review process that said, This wasn't supposed to happen. Why did this happen? What mistakes were made, and should we really be doing this cyber-warfare stuff? And if we're going to do the cyber-warfare stuff again, how do we make sure (a) that the entire world doesn't find out about it, and (b) that the whole world does not fucking collect our source code?"

In September 2011, another piece of malware took to the Web: later named Gauss, it stole information and login credentials from banks in Lebanon, an Iranian ally and surrogate. (The program is called Gauss, as in Johann Carl Friedrich Gauss, because, as investigators later discovered, some internal modules had been given the names of mathematicians.) Three months later, in December, yet another piece of malware began spying on more than 800 computers, primarily in Iran but also in Israel, Afghanistan, the United Arab Emirates, and South Africa. This one would eventually be named Mahdi, after a reference in the software code to a messianic figure whose mission, according to the Koran, is to cleanse the world of tyranny before the Day of Judgment. Mahdi was e-mailed to individuals who worked in government agencies, embassies, engineering firms, and financial-services companies. In some cases, the Mahdi e-mails bore a Microsoft Word file attachment containing a news article about a secret Israeli-government plan to cripple Iran's electrical grid and telecommunications in the event of an Israeli military strike. Other Mahdi e-mails came with PowerPoint files containing slides bearing religious images and text. Anyone who received these e-mails and clicked on the attachment became vulnerable to infection that could result in their e-mails, instant messages, and other data being monitored.

Time started running out for all this malware in 2012, when a man from Mali met with a man from Russia on a spring day in Geneva. The man from Mali was Hamadoun Touré, secretary-general of the International Telecommunication Union, a U.N. agency. He invited Eugene Kaspersky, the Russian C.E.O. of the cyber-security firm Kaspersky Lab, to discuss a partnership to perform forensic analysis on major cyber-attacks—"like a Stuxnet," as Kaspersky recalls. Kaspersky says that Touré made no explicit mention of Iran, even though Stuxnet was an impetus for the collaboration.

The partnership sprang into action within a month of that Geneva meeting, in response to a cyber-attack on Iran that had wiped data from the memory of an unknown number of computers at the country's oil-and-gas ministry. Iranian officials said the cyber-attack, by malware that came to be called Wiper, did not affect oil production or exports, but the ministry reportedly cut Internet access to the national oil company as well as to oil facilities and oil rigs, and to the main sea terminal for oil exports on Kharg Island, for two days.

While investigating the Wiper attack, Kaspersky analysts also discovered Flame, which they announced on May 28, 2012. Kaspersky researchers wrote that Flame appeared to have been state-sponsored and contained elements of Stuxnet's code, suggesting that the makers of both pieces of malware had collaborated in some way. Further evidence that Flame may have been state-sponsored appeared almost immediately after it was made public. At that point, Flame's operators pushed a self-destruction module to the malware, and its command-and-control infrastructure went down. Criminal malware does not delete itself so neatly and so quickly, but intelligence operations generally include "fail-safe" plans to abort if discovered.

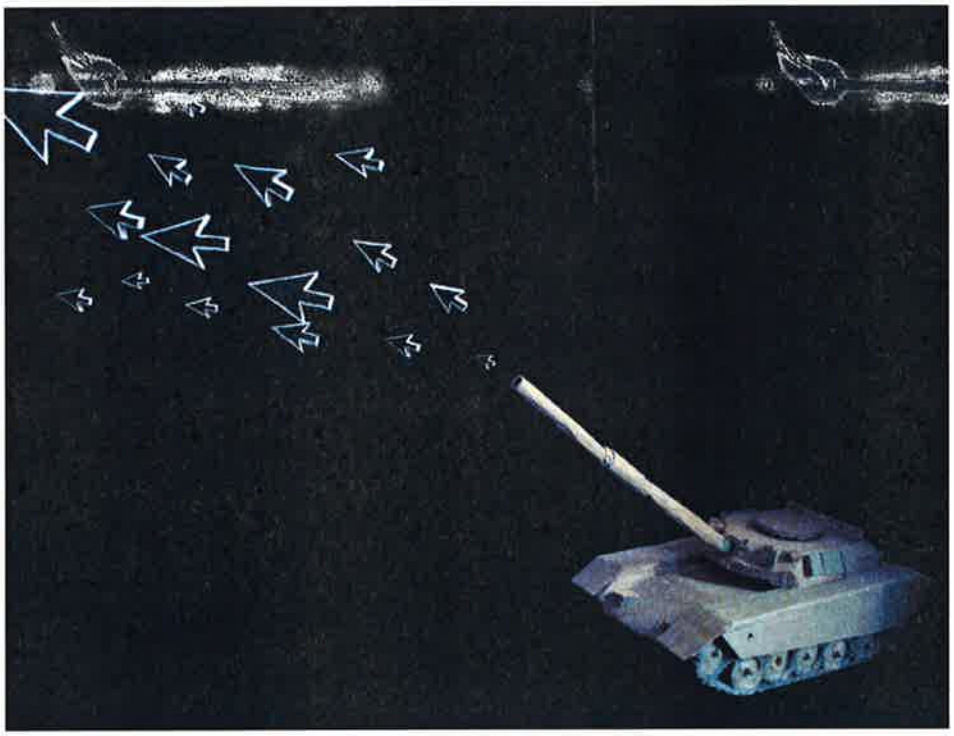
For the next few months, Kaspersky's team was off to the races. It announced Gauss in June and Mahdi in July. In October, it found a much smaller, more targeted version of Flame, called MiniFlame, which had been used to spy on a few dozen computers in Western Asia and Iran, as early as 2007. Traces of some of these pieces of malware were found inside one another. MiniFlame was not only a freestanding program, for instance, but also a module used by both Gauss and Flame, which itself spawned elements of Stuxnet, which was built on the same software platform as Duqu.

Beyond Kaspersky's discoveries, the Iranian press occasionally published news of other cyber-attacks on the country's nuclear program, though none have been independently verified. One person claiming to be an Iranian nuclear scientist e-mailed a prominent researcher in Finland to say that hackers had caused music to play on workstations at full blast in the middle of the night. "I believe it was playing 'Thunderstruck' by AC/DC," the e-mail said.

A small but dedicated group devoured all this news and teased out the possibilities. Wes Brown, who now works as chief architect at ThreatGrid, was struck by Flame's many similarities to his groundbreaking Mosquito program. His first thought upon seeing Flame's code was "It's about time"—it had been two years since he and his buddy brought Mosquito into the world, so he figured that by now, "it was a certainty that a state organization could do what we did."

The man whose company discovered most of this malware, Eugene Kaspersky, became an object of increasing curiosity. One night in January of this year, I arrived for a conversation at his suite in Manhattan's Dream Downtown hotel, where his company was hosting a product launch. Kaspersky answered the door and welcomed me in a way that conveyed two of the qualities—gregarious wonderment and fantastical suspicion—that make him a leading thinker on the topic of cyber-warfare. Still getting dressed, he ducked into his bedroom to button and tuck in his shirt, then summoned me to see a creepy painting on the wall: an extreme close-up of a young woman's face, topped by a Girl

IRAN HAS CREATED A HIGH COUNCIL OF CYBERSPACE AND IS SPENDING $1 BILLION ON CYBER-CAPABILITIES.



Scout cap. The young woman wore big Lolita-style sunglasses. "Terrible," Kaspersky said, shaking his shaggy gray hair. Pointing to the dark sunglasses, he said in broken English that he feared that behind them there were only black holes where the girl's eyes ought to be.

Kaspersky's early education took place at a school supported by the K.G.B., and he and his company have a variety of relationships, both personal and professional, with various Russian-government leaders and agencies. (After one journalist wrote in detail about those connections, Kaspersky accused the journalist of indulging "cold-war paranoia" and responded that, far from being a "spy and Kremlin team member ... the reality however is much more mundane—I'm just a man who's 'here to save the world.' ") But some have wondered if his company's 2012 streak of disclosures was in part politically motivated—all of the spyware Kaspersky made public seems to have advanced U.S. interests and undermined Iranian interests, and many suspect that Iran receives support for its cyber-operations from Russia. Kaspersky denies this, pointing to the company's disclosure of the "Red October" cyber-espionage operation—aimed at governments worldwide—which appears to have been Russian in origin. When it comes to cyber-attacks on Iran, Kaspersky's analysts stop short of explicitly pointing fingers at Washington, but it would seem that sometimes their innuendo obviates the need to name names.

One of the most innovative features of all this malware—and, to many, the most disturbing—was found in Flame, the Stuxnet precursor. Flame spread, among other ways, and in some computer networks, by disguising itself as Windows Update. Flame tricked its victim computers into accepting software that appeared to come from Microsoft but actually did not. Windows Update had never previously been used as camouflage in this malicious way. By using Windows Update as cover for malware infection, Flame's creators set an insidious precedent. If speculation that the U.S. government did deploy Flame is accurate, then the U.S. also damaged the reliability and integrity of a system that lies at the core of the Internet and therefore of the global economy.

Asked whether he sees this development as crossing a Rubicon, Kaspersky raised his hand as if to make a point, brought it back down to his chest, then put his fingers to his mouth and cast his eyes to the side, collecting his thoughts. In an hour-long interview, it was the only question that made him fidget. The response he settled on evoked the moral ambiguity—or, maybe, incoherence—of a cyber-warfare operation such as Flame, which surreptitiously did wrong for the sake of doing right. "It's like gangsters in a police uniform," he finally said. Pressed about whether governments should be held to a higher standard than criminals, Kaspersky replied, "There is no rules for this game at the moment."

III. Boomerang

In June of 2011, someone broke into the computer networks of a Dutch company called DigiNotar. Inside the networks the hacker generated and stole hundreds of digital certificates—electronic credentials that Internet browsers must receive from network servers as proof of a Web site's identity before encrypted data can flow back and forth between a computer and the site. Digital certificates had been stolen before but never in such quantity. Whoever was behind the DigiNotar hack could have broken into other networks and used the stolen certificates to intercept Web traffic anywhere and to conduct surveillance on anyone. They could have stolen information worth millions of dollars or unearthed the secrets of some of the world's most powerful people. But instead, for two months, the hackers who controlled DigiNotar's certificates, apparently in Iran, conducted "man in the middle" attacks on Iranian connections to and from sites including Google, Microsoft, Facebook, Skype, Twitter, and—notably—Tor, which provides anonymizing software that many dissidents in Iran have used to elude state surveillance. The hackers were intent on intercepting the e-mails, passwords, and files of ordinary Iranians.

A 21-year-old in Tehran who goes by the name of Comodohacker took responsibility for the DigiNotar breach. In an online posting, he claimed the hack was revenge for an episode in the Balkan wars when Dutch soldiers surrendered Muslims to Serb militias; the Muslims were summarily executed. But the scale and focus of this event—in one month alone, 300,000 people in Iran who connected to Google were vulnerable to hacking via stolen DigiNotar certificates—led many to believe that the Iranian government had engineered the DigiNotar breach itself, using Comodohacker as camouflage. One analyst who spent months investigating the event scoffs at the young man's claim of responsibility. "Twenty-one-year-old hackers are the new stealth," he says—meaning that militaries use hackers to hide their operations the same way they use advanced design to hide bombers. (After details of the DigiNotar hack were made public, the company went bankrupt.)

The U.S. began cultivating cyber-capabilities as an adjunct to its diplomatic, intelligence, and military operations. Iran's initial impetus was to suppress domestic dissent, especially in the wake of the 2009 Green Revolution protests, when citizens took to the streets to dispute the re-election of President Mahmoud Ahmadinejad. But ever since the Stuxnet attack, Iran has been enhancing its cyber-warfare capability. Public remarks by government leaders in March 2011 indicated that the Iranian Revolutionary Guard had created a cyber unit to coordinate offensive attacks on "enemy sites." In March 2012, Ayatollah Ali Khamenei established the High Coun-

CONSTRUCTION BY STEPHEN DOYLE

cil of Cyberspace; reportedly, Iran is spending $1 billion on building cyber-capabilities.

Asymmetric warfare—unconventional, guerrilla-style attacks on more powerful adversaries, such as the U.S.—is a cornerstone of Iranian military doctrine. The Revolutionary Guard has ties to terrorist organizations and to prominent hacker groups both in Iran and around the world. Iran may be receiving support for its cyber-operations not only from Russia but also from China and the terrorist network Hezbollah. A top hacker with many well-placed friends in the U.S. government says, "I hear Iran pays Russian guys millions to do the attacks, and the guys are living high, flying in prostitutes from all over." Who told him this? "Nobody who would talk to you," he says. Other dramatic but plausible speculation abounds. One high-level Lebanese political operative believes that the Revolutionary Guard runs its cyber-operations from a six-story underground bunker in a Hezbollah-controlled neighborhood of Beirut called Haret Hreik. Lebanon's absence of any laws against cyber-crime or hacking would make it an appealing launching pad for operations. "Consider how Iran uses Hezbollah as a platform for many critical activities," the Lebanese operative notes. "We say, 'Lebanon is the lungs through which Iran breathes.' Iran wouldn't breathe these attacks with its own lungs. They need a way to answer Stuxnet without having to answer *for* what they are doing. Hezbollah is the way."

As recently as February of 2012, U.S. defense officials privately dismissed Iran's cyber-warfare efforts as trifling. By August, many had come to believe that the ARAMCO hack showed that Iran was learning fast. In essence, the ARAMCO attack was a mirror image of what had happened when Wiper shut down Kharg Island. Before ARAMCO, Kharg had been the only major cyber-attack on record whose goal was to annihilate data rather than to steal or alter it. The worm that struck ARAMCO, named Shamoon (a word found in the program, the Arabic version of the proper name Simon), adopted this same tactic. Kaspersky believes that Shamoon was a copycat, inspired by the Kharg Island hack. In its attack technique, if not in its actual code, Shamoon anticipates the well-known boomerang effect in weaponry: adaptation and re-deployment of a weapon against the country that first launched it.

Two weeks after the ARAMCO attack, Qatar's state-owned natural-gas company, RasGas, was also hit by malware. Unconfirmed reports say that the cyber-weapon used was also CONTINUED ON PAGE 123

Much Ado in Santa Monica

In Joss Whedon's film of *Much Ado About Nothing*—Shakespeare's witty battle of the sexes—Amy Acker, as Beatrice, takes a showstopping pratfall down a flight of stairs. "That was Joss's idea," she says. At 36, she's a seasoned native of the "Whedonverse," having been cast more than a decade ago in Whedon's *Buffy the Vampire Slayer* spin-off series, *Angel,* and most recently in his 2012 horror film, *The Cabin in the Woods.* But the actress, who is married and has two children, is also a seasoned Shakespearean: her first stage job out of college, in fact, was playing Hero in *Much Ado About Nothing.* "I would be lying to say I didn't dream of playing Beatrice," she says now. Acker's *Angel* co-star Alexis Denisof plays Benedick. They read the parts together several years ago at Whedon's house, and in 2011, when the writer-director-producer decided to make a no-budget screen adaptation on a break from *The Avengers,* Acker and Denisof were the first people he contacted. "We really had no idea what was happening," says Acker. "I was kind of thinking I would show up and Joss would have his Flip cam or his iPhone and it would be like a glorified reading and we would film it." Instead, Whedon and his wife, Kai Cole, turned their Santa Monica home into a set, and the costumes and props (town cars, iPods, walkie-talkies) are decidedly 21st-century. In the end, Acker says, the 12-day shoot came down to "people who love each other getting together and doing a project that they're passionate about." —CALLIE WRIGHT

STYLED BY DEBORAH AFSHANI; HAIR PRODUCTS BY ORIBE; MAKEUP PRODUCTS BY NARS; NAIL ENAMEL BY SHESWAI LACQUER; HAIR BY KRISTEN SHAW; MAKEUP BY JENNA ANTON; MANICURE BY DEBBIE LEAVITT; PRODUCED ON LOCATION BY VIEWFINDERS; FOR DETAILS, GO TO VF.COM/CREDITS

PHOTOGRAPH BY HASSE NIELSEN

not come through to the other side, and died an alcoholic. During that Paris fashion season two years ago, on March 6, 2011, the day of the Galliano fall/winter women's ready-to-wear show, I couldn't be there because I had flown to Edinburgh to be at the stone setting for my brother's grave, which is in the Piershill Cemetery, in a section designated for Jews, which is what our family is. It was drizzling, cold, miserable. When I got back to Paris that night, the people who had been at the Galliano show, earlier that day, reported that it too had seemed funereal, there was such a sense of pain about Galliano's fall.

Somehow my private grief and the public sadness that was so visceral all that week dovetailed in a way that seemed right to me. When Sidney Toledano got up on the runway at the Dior show, it wasn't just to handle a P.R. emergency. It was to address the collective pain and also the personal pain he felt—as if something horrible had happened to a family member, which essentially it had. That Galliano had catalyzed such intense feeling was sadly, ironically appropriate, because emotion in fashion is a subject he stressed from the beginning; it's why people have cared so much about his clothes.

In fact, he was preparing to teach a four-day workshop on the subject to students at Parsons in New York this past May. He had already taught a similar class in March at his alma mater, Central Saint Martins—a grand success. But at the eleventh hour the Parsons class was canceled. Some students had begun petitioning and protesting against Galliano's appearance, and so the school asked him to submit to a mass question-and-answer session in the school's auditorium. It had the potential to turn into a show trial, and his publicist—correctly, I thought—refused to put the designer through that. Galliano's trial should be over. Now it's time for him to get out the scissors. And ribbons. □

FROM THE ARCHIVE

For these related stories, visit VF.COM/ARCHIVE

- **John Galliano begins his reign at Givenchy** *(Cathy Horyn and Karl Lagerfeld, January 1996)*
- ***V.F.*'s "My Dream": John Galliano** *(December 2010)*

Cyber-War

CONTINUED FROM PAGE 104 Shamoon. Qatar, home to three U.S. military bases, is among America's closest allies in the Middle East and, therefore, another convenient proxy target.

During the second week of September 2012, a new spate of cyber-attacks against American interests began. This time, the targets were on American soil: U.S. banks. A previously unknown group calling itself the Izz ad-Din al-Qassam Cyber Fighters and presenting itself as an organization of Sunni jihadists made an online posting written in broken English, referring to an anti-Islamic video on YouTube called "Innocence of Muslims" that had sparked riots in the Muslim world the week before. The posting stated that "Muslims must do whatever is necessary to stop spreading this movie.... All the Muslim youths who are active in the Cyber world will attack to American and Zionist Web bases as much as needed such that they say that they are sorry about that insult."

If Qassam really were a Sunni jihadist group, then Iran, a predominantly Shiite nation, would hardly have been involved. But the jihadist flavoring appears to be a false flag. As one U.S. intelligence analyst points out, none of the language used in Qassam's public communication bears any resemblance to the standard language of jihadist groups. There was no trace of Qassam's formation in any Sunni, jihadist, or al-Qaeda online forums. And the name Qassam itself refers to a Muslim cleric who has significance for Palestinians and Hamas but not for jihadists. "Everything is wrong," this analyst says. "It looks manufactured."

Qassam announced that it would inundate Bank of America and the New York Stock Exchange with distributed-denial-of-service (DDoS) attacks. Such attacks seek to crash a Web site or induce the failure of a computer network by making an overwhelming number of requests for connections. Qassam proceeded to expand its targets to include many more banks, including SunTrust, Regions Financial, Webster Financial Corporation, JPMorgan Chase, CitiGroup, Wells Fargo, U.S. Bancorp, Capital One, PNC, Fifth Third Bank, HSBC, and BB&T. Qassam knocked at least five of these banks' Web sites off-line, though most of the banks have said that no money or information was stolen. In October, PNC bank C.E.O. James Rohr stated that "we had the longest attack of all the banks" and warned that "cyber-attacks are a very real, living thing, and if we think we are safe that way, we're just kidding ourselves." Shortly afterward, the attacks on PNC escalated, causing further problems. Neither Rohr nor any other high-level executive of any victim bank has since made any such conspicuous and pointed statement. "The lesson from Rohr's statement was, don't talk," says one former national-security official.

As an attack technique, DDoS is primitive, and the impact is usually evanescent. But the difference between Qassam's DDoS and previous attacks was like the difference between a crowded parking lot at the mall and a full-on, road-rage-inducing L.A. traffic jam on Memorial Day weekend. Qassam's DDoS was especially effective—and, for its victims, especially damaging—because it hijacked entire data centers full of servers to do its work, generating 10 times more traffic than the largest hacktivist DDoS previously recorded. (That was Operation Avenge Assange, launched by Anonymous in defense of Wikileaks, in December 2010.)

To absorb the gargantuan volume of traffic coming their way, banks had to buy more bandwidth, which telecommunication companies had to create and provide. Telecoms have borne the brunt of these battles, just as the banks have, spending large sums to expand their networks, and to strengthen or replace hardware associated with their "scrubber" services, which absorb DDoS traffic. Qassam's first wave of attacks was so intense that it reportedly broke the scrubbers of one of this country's largest and best-known telecom companies. In December, AT&T executive director of technology security Michael Singer reportedly stated that the attacks posed a growing threat to the telecommunications infrastructure, and that the company's chief security officer, Ed Amoroso, had reached out to government and peer companies to collaborate in defending against the attacks. Neither Amoroso nor any of his peers have provided specific information about the damage done or the exact cost to telecom companies. (Amoroso declined to comment.)

Qassam Cyber Fighters, like Comodohacker and the Cutting Sword of Justice, launched attacks that were technically unsophisticated enough that they could have been executed by any talented hacktivist or criminal group. But the context, timing, techniques, and targets of Qassam's DDoS all but implicate Iran or its allies. The unpublished research of one cyber-security analyst provides some concrete though circumstantial evidence connecting the bank attacks to Iran. A few weeks prior to the start of the attacks, in September, several individual hackers in Tehran and an Iranian hacker living in New York bragged of having created the same kind of attack tools that Qassam would use. The hackers made postings online offering those tools for sale or rent. The postings were then mysteriously deleted. A hacker in Iran who appeared to be the prime mover in this group goes by the name of Mormoroth. Some of the information concerning these attack tools was posted to his blog; the blog has since disappeared. His Facebook page includes pictures of himself and his hacker friends in swaggering poses reminiscent of *Reservoir Dogs.* Also on Facebook, his hacking group's page bears the slogan "Security is like sex, once you're penetrated, you're fucked."

Communications from Qassam have been traced to a server in Russia that had only once previously been used for illicit activity. This might indicate that Qassam's attacks were planned with greater care and deliberateness than is typical of hacktivist or criminal intrusions, which usually come from servers where illicit activity is common. This I.P. address, however, like almost all tracebacks of Web traffic, could easily have been faked. Whoever they are, the Qassam Cyber Fighters have a sense of humor. Some of the computers they leveraged for use in the bank attacks were located inside the U.S. Department of Homeland Security.

Critically, two other things distinguish Qassam, according to an analyst who works for several victim banks. First, each time the banks and Internet-service providers figure out how to block the attacks, the attackers find a way around the shields. "Adaptation is atypical," he says, and it may indicate that Qassam has the resources and support more often associated with state-sponsored hackers than with hacktivists. Second, the attacks appear to have no criminal motive, such as fraud or robbery, suggesting that Qassam may be interested more in making headlines than in causing truly meaningful harm. The researcher points out that, for all the hassle and financial damage Qassam has caused its victims, its main accomplishment has been to make news pointing up American weakness in the cyber realm at a time when the U.S. wants to demonstrate strength.

The U.S. banking leadership is said to be extremely unhappy at being stuck with the cost of remediation—which in the case of one specific bank amounts to well over $10 million. The banks view such costs as, effectively, an unlegislated tax in support of U.S. covert activities against Iran. The banks "want help turning [the DDoS] off, and the U.S. government is really struggling with how to do that. It's all brand-new ground," says a former national-security official. And banks are not the only organizations that are paying the price. As its waves of attacks continue, Qassam has targeted more banks (not only in the U.S., but also in Europe and Asia) as well as brokerages, credit-card companies, and D.N.S. servers that are part of the Internet's physical backbone.

For a major bank, $10 million is a drop in the bucket. But bank executives, and current and former government officials, see the recent attacks as shots across the bow: demonstrations of power and a portent of what might come next. One former C.I.A. officer says of the conflict thus far, "It's like the fingernail full of coke, to show that you're dealing with the real thing." Of the bank attacks in particular, a former national-security official says, "If you're sitting in the White House and you can't see that as a message, I think you're deaf, dumb, and blind."

Another hack, which occurred even as the bank attacks continued through the spring, delivered a still more dramatic financial threat, although its ultimate source was difficult to discern. On April 23, the Twitter account of the Associated Press sent this message: "Breaking: Two Explosions in the White House and Barack Obama Is Injured." Faced with this news, the Dow Jones Industrial Average dropped 150 points—the equivalent of $136 billion in value—within a matter of minutes. Upon learning that the information was false—and that the A.P.'s Twitter account had simply been hacked—the markets rebounded. A group calling itself the Syrian Electronic Army (S.E.A.) claimed credit for the disruption.

But did the S.E.A. act alone? Previously, the S.E.A. had hacked the Twitter accounts of several other news organizations, including the BBC, Al Jazeera, NPR, and CBS. But none of its hacks had taken aim at, or caused any collateral damage to, the U.S. financial system. That distinction had previously belonged only to the Qassam Cyber Fighters, who, as noted, likely have Iranian ties.

One Middle Eastern cyber-analyst in London has said that "there are strong indications that members of [S.E.A.] are trained by Iranian experts." And an American analyst pointed out that the A.P. hack—which used information warfare to cause financial damage—not only resembles Qassam's technique but also mirrors Iran's own perception of what the U.S. has done to the Islamic Republic. (Last year, before Qassam began its attacks on the banks, state-run Iranian media asserted that the U.S. had driven Iran's currency to the brink of collapse by telling lies about Iran.) At this point, there's no solid evidence that Iran was party to the A.P. hack, but among the list of plausible scenarios, none is comforting. Perhaps, with Iran's help or urging, the S.E.A. continued Qassam's experimentation with threats on the U.S. financial system. Perhaps the S.E.A. learned from Qassam's bank attacks and launched an independent operation on the same model. Or perhaps whoever hacked the A.P. had no financial outcome in mind at all—it was just a $136 billion aftershock.

IV. The Cyber-Arms Bazaar

Throughout the fall and winter of 2012, U.S. officials began to speak more frequently than usual about cyber-war. During the same period, Iranian officials offered unusually detailed accusations regarding Western sabotage. On September 17, an Iranian official claimed that power lines to its nuclear facility at Fordow had been damaged, perhaps by Western "terrorists and saboteurs." The next day, the bank attacks commenced, and State Department chief counsel Harold Koh stated for the record that the Obama administration believes the law of war applies to cyber-operations. He emphasized that "civilian objects . . . under international law are generally protected from attack." The following week, Iran claimed that the German manufacturer Siemens had planted tiny explosives inside some of the hardware used for its nuclear program. Siemens denied any involvement. Then Western intelligence sources let *The Sunday Times* of London know that another explosion had occurred at Fordow. This time, a spying device disguised as a rock blew up when Iranian soldiers tried to move it.

In the subsequent months, as the bank attacks continued, the U.S. and Iran appeared to engage in a kind of semi-public tit for tat. In November, a classified Presidential Policy Directive was leaked to *The Washington Post;* the directive allowed the military to take more aggressive steps to defend computer networks in the U.S. In December, Iran conducted a cyber-warfare drill during its naval exercises in the Strait of Hormuz, to demonstrate the resilience of its submarines and missiles to cyber-attack. In January 2013, Pentagon officials reportedly approved a fivefold increase in the number of U.S. Cyber Command personnel, from 900 to 4,900, over the next few years. An Iranian general, as if in response, noted publicly that the Revolutionary Guard controls "the fourth largest cyber army in the world."

In the midst of all this, the Pentagon's secretive research-and-development wing, the Defense Advanced Research Projects Agency (DARPA), invited hackers to propose "revolutionary technologies for understanding, managing, and planning cyberwarfare," for use in a new effort called "Plan X." Plan X aims to persuade some of the most talented hackers in the country to lend the Pentagon their skills. The best talents in cyber-security tend to work in the private sector, partly because corporations pay better and partly because many hackers lead unconventional lives that would clash with military discipline. Drug abuse, for instance, is so common in the hacking subculture that, as one hacker told me, he and many of his peers could never work for the government or the military, because "we could never get high again."

For at least a decade, Western governments—among them the U.S., France, and Israel—have been buying "bugs" (flaws in computer programs that make breaches possible) as well as exploits (programs that perform jobs such as espionage or theft) not only from defense contractors but also from individual hackers. The sellers in this market tell stories that suggest scenes from spy novels. One country's intelligence service creates cyber-security front companies, flies hackers in for fake job interviews, and buys their bugs and exploits to add to its stockpile. Software flaws now form the foundation of almost every government's cyber-operations, thanks in large part to the same black market—the cyber-arms bazaar—where hacktivists and criminals buy and sell them. Some of this trade is like a floating craps game, occurring at hacker conventions around the globe. At gatherings such as Def Con in Las Vegas, dealers in bugs and exploits reserve V.I.P. tables at the most exclusive clubs, order $1,000 bottles of vodka, and invite top hackers to hang out. "It's all about the relationships, all about the drinking," says one hacker. "This is why government needs the black market: you can't just call up someone in the sober light of day and say, Can you write a bug for me?" The most talented hackers—smartest guys in the room, to a man—are egged on and beckoned to devise ever more ingenious intrusion capabilities, for which someone, somewhere, is always willing to pay.

In the U.S., the escalating bug-and-exploit trade has created a strange relationship between government and industry. The U.S. government now spends significant amounts of time and money developing or acquiring the ability to exploit weaknesses in the products of some of America's own leading technology companies, such as Apple, Google, and Microsoft. In other words: to sabotage American enemies, the U.S. is, in a sense, sabotaging its own companies. None of these companies would speak on the record about the specific issue of U.S.-government use of flaws in their products. Speaking more generally about the use of flaws in Microsoft products by many governments, Scott Charney, head of Microsoft's Trustworthy Computing Group, points out that nations have been conducting military espionage from time immemorial. "I don't expect it to stop," he says, "but governments should be candid that it is going on and have a discussion about what the rules should be." More openly defining what is legitimate for military espionage and what is not would be constructive. This would bring order to the mess of outdated laws and contradictory cultural precepts that aggravate the uncontrollable, unintended consequences of cyber-operations by nation-states. Brad Arkin, Adobe's chief security officer, says, "If you drop a bomb, you use it once and then it's done, but an offensive exploit in the digital realm, once it's used, it's out there.... Regardless of what [its initial intended] use was, it very quickly rolls downhill." First, he explains, it's "used by nation-states for espionage, and then you see it quickly go towards the financially motivated, and then to the hacktivists, whose motivations are hard to predict."

Meaningful discussion of U.S. cyber-warfare continues to take place behind veils of secrecy that make the drone program look transparent. President Obama, who has defended American use of drones, has never spoken about offensive cyber-warfare. The leak of information about Stuxnet has only driven that conversation further underground. "Our bureaucracy confirms what our elected officials are unwilling to acknowledge," says one former intelligence officer, regarding the F.B.I.'s leak investigation into Stuxnet, which no government entity has officially claimed as a U.S. project. "It's absurd."

Fundamentally, cyber-warfare is a story about proliferation. Iran's nuclear program crossed a line that Israel and the U.S. deemed unacceptable, so the U.S. and its allies used a secret new weapon to try to stop it. With Stuxnet becoming public, the U.S. effectively legitimized the use of cyber-attacks outside the context of overt military conflict. Stuxnet also appears to have emboldened Iran to mount attacks on targets of its choosing. One former government official says, "What did we anticipate that Iran's reaction [to Stuxnet] was going to be? I bet it wasn't going after Saudi ARAMCO."

The paradox is that the nuclear weapons whose development the U.S. has sought to control are very difficult to make, and their use has been limited—for nearly seven decades—by obvious deterrents. In the years since August 1945, a nuclear weapon has never been used in war. Cyber-weapons, by contrast, are easy to make, and their potential use is limited by no obvious deterrents. In seeking to escape a known danger, the U.S. may have hastened the development of a greater one.

And unlike the case with nuclear weapons, anyone can play. Wes Brown, who has never sold a bug or exploit to a government but whose Mosquito program may have inspired part of the best-known cyber-warfare operation so far, puts it simply. "You don't have to be a nation-state to do this," he says. "You just have to be really smart." □

FROM THE ARCHIVE

For these related stories, visit VF.COM/ARCHIVE

- **The Web as worldwide battleground** *(Michael Joseph Gross, May 2012)*
- **China's hack attack on America's intellectual property** *(Michael Joseph Gross, September 2011)*
- **When the Stuxnet worm went global** *(Michael Joseph Gross, April 2011)*

Channing Tatum

CONTINUED FROM PAGE 71 I was broke, a vagabond. I did it because it was fun. We say a line in [*Magic Mike*]: 'It's girls, money, and a good time.' That's all you need for an 18- or 19-year-old. I liked the dancing." Speaking specifically of Club Joy, he said, "The getting-naked part was hard. You see some kids, all they want to do is get naked."

Tatum burned out—it came in the way of an epiphany, late one night, in a side street or alley. He turned left when he should have turned right, and there was the abyss, yawning before him, and in it he saw himself 5 or 10 years down the line, faded, gone to seed, but still shaking that thing, G-string stuffed with greasy bills. *Goddammit,* he told himself. *I've got to get outta here.*

Magic Man

He went to Miami. You can picture him walking up and down the Cuban avenues beside the sea, making eye contact, speaking to strangers. He knew none of the rules. "In my infinite knowledge, I thought Miami was going to be a smart choice to get away from the partying and shit of Tampa," he told me. "I could get a job in a business and work my way up. That was my idea."

One afternoon, an older man approached Tatum on the street—imagine a raincoat-on-a-sunny-day type. He asked if Channing had "representation." When Chan shrugged, the man said, *Look, a kid like you, who looks like that, could be a model and needs only an older man to teach and guide you for the dollars to start rolling in. It just so happens the relevant documents are back in my apartment, if you'll just come with me . . .* "He was creepy," said Tatum, "and actually he did end up to be just a complete creep, trying to, like, fuck me, and I was like, 'All right, man,' but it piqued my interest." The next day, or maybe a few days later, Chan walked into a legitimate modeling agency and presented himself as Joe Buck presented himself to the denizens of Times Square, with an air of "Here I am. What are you gonna do with me?"

Tatum was signed up; his face and body were photographed, and the photos were