FROM RUSSIA WITH MALWARE

RUSSIAN HACKERS ARE THE MOST SOPHISTICATED AND INVENTIVE IN THE WORLD, AND THE KREMLIN KNOWS HOW TO DEPLOY THEM

By **OWEN MATTHEWS**
Illustration by **OLIVER MUNDAY**

Як
130

In hacker jargon

it's called a "cyber-to-physical effect." It's when a hacker reaches out from the virtual world into the real one—often with catastrophic consequences. The Americans and Israelis pioneered the technique back in 2009 when the Stuxnet program infiltrated Iranian computer systems and wrecked thousands of uranium-enriching centrifuges. But now other players—especially the Russians and Chinese—are getting into the game of remotely using computer networks to destroy infrastructure and threaten human lives. Last year, according to a report by Germany's Federal Office for Information Security, a blast furnace melted down in an unnamed industrial city in Germany after a digital attack on its control systems, causing "massive damage."

It nearly happened in the United States too, when unknown hackers succeeded in penetrating U.S. electrical, water and fuel distribution systems early in 2014. While old-fashioned, relatively low-tech data hacks make headlines—for instance, high-profile break-ins over the last 12 months to the email systems and databases of the White House, State Department, Department of Homeland Security, Department of Defense and Sony Pictures Inc.—what has security officials seriously worried is the new and dangerous world of cyber-to-physical infrastructure attacks.

"This is not theoretical," National Security Agency Director Admiral Michael Rogers told the U.S. House of Representatives' Intelligence Committee recently. Hacking attacks on the U.S. and its allies are "costing us hundreds of billions of dollars," Rogers warned, and will result in "truly significant, almost catastrophic failures if we don't take action."

According to Alexander Klimburg, an affiliate of the Harvard Kennedy School of Government's Belfer Center and senior research fellow at the Hague Centre for Strategic Studies, "cyberspace today is like Europe in 1914, before World War I. Governments are like sleepwalkers. They do not comprehend the power of new technology and the consequences of misunderstanding each other's activities."

According to the U.S. Intelligence Community's 2015 "Worldwide Threat Assessment" report, Russia and China are the "most sophisticated nation-state actors" in the new generation of cyberwarfare, and Russian hackers lead in terms of sophistication, programming power and inventiveness. "The threat from China is overinflated, while the threat from Russia is underestimated," says Jeffrey Carr, head of Web security consultancy Taia Global and author of the book *Inside Cyber Warfare*. "The Russians are the most technically proficient. For instance, we believe that Russian hackers-for-hire were responsible for the Sony attack."

Last year hackers gained access to thousands of Sony company emails and threatened further damage unless a film lampooning North Korean leader Kim Jong Un was withdrawn from cinemas. "We spoke to [one of the hackers] via an intermediary," says Carr. "Even after Sony lost 80 percent of its network capability, the hackers were still operating. That shows an incredibly high level of technical ability."

KRIS TRIPPLAAR/SIPA USA/AP

NCCIC
NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER
US-CERT / NCCI / US-CERT
Last 24 Hours
Last 7 Days
U.S. DEPARTMENT OF HOMELAND SECURITY

+ CYBER PRESIDENT: Barack Obama speaks at the National Cybersecurity and Communications Integration Center in January.

KRIS TRIPPLAAR/SIPA USA/AP

The Moscow connection is worrying because Russia is the only country to date to have combined cyberwarfare with assaults by conventional guns and tanks. "The Russia-Georgia war of 2008 was a perfect example of a combined kinetic and cyber operation," says Carr. "Nobody else has ever done anything like that."

Similarly, in the wake of Russia's annexation of Crimea in April 2014, ground assaults were accompanied by a deluge of mostly low-tech cyberassaults on over a hundred government and industrial organizations in Poland and Ukraine, as well as attacks on the European Parliament and the European Commission. Many of these attacks featured a modified version of "BlackEnergy," a kind of malware program known as a Trojan horse that is designed to remotely take over computers. A network of such infected computers, or "bots," is known as a "botnet." This can be mobilized to overwhelm a target server with requests for information and crash it—an attack known as Distributed Denial of Service, or DDoS.

"The BlackEnergy malware was authored by a Russian hacker and originally used for DDoS attacks, bank frauds and spam distribution," says Pierluigi Paganini, founder of the Security Affairs blog and a member of a European Union Agency for Network and Information Security working group. "But the new variant was used in targeted attacks on government entities and private companies across a range of industries."

One of the biggest mysteries of the latest generation of cyberattacks—known in the U.S. government as Offensive Cyber Effects Operations—is working out who is behind them and whether they are being launched with political or criminal intent.

"CYBERSPACE TODAY IS LIKE EUROPE IN 1914, BEFORE WORLD WAR I. GOVERNMENTS ARE LIKE SLEEPWALKERS. THEY DO NOT COMPREHEND THE POWER OF NEW TECHNOLOGY."

What's not in doubt is that Russian hackers have long been kings of the cybercrime world. A group of Russians and Ukrainians were named by U.S. federal prosecutors as being behind the biggest cybercrime case in U.S. history, a bank-card fraud spree from 2010 to 2013 that cost companies including JetBlue, J.C. Penney and French retailer Carrefour more than $300 million. A group of Russian "click-jackers" were convicted in the U.S. last year for hijacking users of Apple's iTunes store, Netflix, the U.S. Internal Revenue Service, Amazon.com, ESPN.com and the *Wall Street Journal* website—as well as computers at NASA.

Another as-yet-unidentified hacking ring, based in a small city in south-central Russia, stole some 1.2 billion Internet logins and passwords and more than 500 million email addresses last year by plundering data from more than 400,000 websites, according to U.S. cybersecurity firm Hold Security. And in February the Moscow-based Internet security company Kaspersky Labs revealed details of the biggest Internet heist of all time—a raid on over 100 banks in Russia, Ukraine, Japan, the United States and Europe from 2013 to 2014. Kaspersky reported seeing evidence of $300 million in losses just from the banks that had hired it to clean up the mess—and estimated that the total amount stolen was likely to be around $900 million.

"This is cybercrime on an industrial scale," says one Moscow-based Western Internet security consultant, who helped overhaul several Russian banks' defenses in the wake of the attack. "In one case in Kiev, they made the bank's ATMs spew out money, which was collected by people walking by." The techniques used to break into the bank's electronic systems via flaws in Adobe and Microsoft programs "were not particularly sophisticated," says the consultant, "but it was amazing how careful they were not to alert the victims and to keep their backdoor into their systems a secret."

The exact nature of the links between these criminal hackers and the Russian government remains murky. "Cybercrime, cyberterrorism and cyberwarfare share a common technological basis, tools, logistics and operational methods," says Klimburg. "They can also share the same social networks and have comparable goals. The differences between these categories of cyberactivity are often razor–thin. It's hard to distinguish in cyberspace between financial and political motivation."

In particular, the methods of delivering malware into a target computer are identical. Hackers seek vulnerabilities in popular programs that allow them to introduce alien code, in particular a weak spot in the code known as a "zero-day," meaning it remains unpatched and can be used for an attack before it is discovered by everyone else, so there are zero-days between an attack and the discovery of the vulnerability. A good zero-day vulnerability can be sold for $200,000, says Klimburg, but there are many examples of Russian hackers "lending" their zero-day hacks to the government for espionage purposes, then using them for crime later.

"Hundreds of 'black-hat' Russian hackers are doing this for a living—whether it's at the order of Swiss bankers or Ukrainian oligarchs," says Carr. "Russian hackers who are caught are given the choice to work for the FSB [Federal Security Service] or to go to jail. The FSB also has some on contract hire."

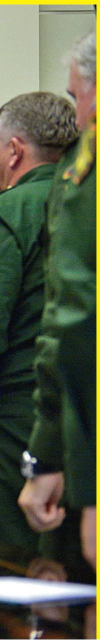
There is strong evidence, going back to cyberattacks on Estonia as early as 2007, that Russian cybercriminals were working either with or for the Russian state. But now, it seems, the Kremlin is getting directly involved. U.S. Director of National Intelligence James Clapper told the Senate Armed Services Committee in March that Russia's Ministry of Defense is "establishing its own cybercommand" responsible for "conducting offensive cyberactivities." And the Russian government appears to be stepping up funding for the research and development of cybertechnology at world-class computer science centers such as the prestigious St. Petersburg Polytechnic University and Samara State University, according to information gathered by Seattle-based Taia Global.

LEFT: ALEXEI DRUZHININ/RIA NOVOSTI/KREMLIN/REUTERS; RIGHT: KIRILL KUDRYAVTSEV/AFP/GETTY

Possible evidence linking recent hacking attacks on the U.S. government to the Russian state includes the digital signatures of a hacker group known as Advanced Persistent Threat 28 (or APT28, identified by the U.S.-based Internet security company FireEye) and a family of hackers labeled CozyDuke, CosmicDuke, MiniDuke and OnionDuke (spotted by Kaspersky Labs). These groups, which may or may not be related, have some giveaway signatures that tie them to Russia. "Indicators in APT28's malware suggest that the group consists of Russian speakers operating during business hours in Russia's major cities," says a recent FireEye report. "More than half of the malware samples...attributed to APT28 included Russian-language settings."

But the real giveaway is not the forensics of the APT28 codes but their targets over the past five years, which have included Georgia's ministries of internal affairs and defense, the Polish and Hungarian governments, NATO, the Organization for Security and Co-operation in Europe, the Norwegian army and U.S. defense contractors. The APT28 hacking crew "does not appear to conduct widespread intellectual property theft for economic gain, but instead is focused on collecting intelligence," says FireEye.

PUTIN'S ARMY: After reports that Russia was behind hacking attacks on the White House this year, Kremlin spokesman Dmitry Peskov, above, said blaming Russia had become a sport, adding: "At least they haven't looked for Russian submarines in the Potomac."



LEFT: ALEXEI DRUZHININ/RIA NOVOSTI/KREMLIN/REUTERS; RIGHT: KIRILL KUDRYAVTSEV/AFP/GETTY

"That would be most useful to a government."

Though there is evidence that the development teams of APT28 and the CosmicDuke, MiniDuke and OnionDuke "worked together and shared same knowledge and coding techniques," and that they all have Russian origins, it's likely they are separate groups, says Paganini. "All these groups are state-sponsored hackers, probably backed by the Russian government, though it is likely that they operate under different divisions of the same cyberarmy."

Was APT28—and the Kremlin—behind hacking attacks on the White House and State Department this year, which cracked open confidential email records (though not, according to a spokesman, the president's personal email)? The Kremlin strongly denies it. "We know that blaming Russia for everything has turned into a sport," Kremlin spokesman Dmitry Peskov joked to journalists. "At least they haven't looked for Russian submarines in [Washington's] Potomac River, as has been the case in a few other countries."

Yet some code—in particular, the family of "backdoors" into programs known as CHOPSTICK—that is frequently used by APT28 has been linked to those virtual break-ins. And there's less ambiguity about a similar attack on an unclassified military network at the U.S. Department of Defense last year. "We analyzed their network activity, associated it with Russia and then quickly kicked them off the network," Secretary of Defense Ashton Carter said in April.

Cyberspying on the West Wing's emails may be cheeky, but it's not much different from the old-school espionage and signals-intelligence games that Russia and America have been playing for decades. What's truly scary, on the other hand, is infiltrating physical infrastructure in a way that could herald a new generation of violent covert action and sabotage. "This is an entirely new way of waging war," says one former KGB general once posted as a spy to London who now works in the private security sector. "It is like the invention of planes or submarines. Suddenly you can attack the enemy from a completely new and unexpected direction.... This is the essence of warfare: constant surprise."

In April, Eugene Kaspersky, the Moscow-born CEO of Kaspersky Labs, noted that there has been a dramatic surge in targeted attacks against power grids, banks and transportation networks around the world—and warned that groups targeting crucial infrastructure have "the capacity to inflict very visible damage. The worst terrorist attacks are not expected."

Among the most frightening new-generation cyberweapons are those designed to target super-secure, so-called "air-gapped" systems that have no links to the Internet or outside networks. The developers of Stuxnet bridged the air gap by developing ingenious programs that infected CD-ROMs and memory sticks that then colonized Iran's nuclear development computers, ultimately inflicting devastating physical damage on uranium centrifuges and forcing the Iranians to replace their entire computer infrastructure. But a Stuxnet-like program that can be carried by email and memory sticks, called Uroburos, has been around since 2011—and was diagnosed as being of Russian origin. Uroburos targets Microsoft Windows, sets up surreptitious communications with its parent network and is able to leap across air gaps isolating secure networks from the Internet.

"WE BELIEVE THAT RUSSIAN HACKERS-FOR-HIRE WERE RESPONSIBLE FOR THE SONY ATTACK."

"The scary thing is that now everyone can do pretty much anything to anyone," says Klimburg. He believes that one way to distinguish between criminal and government cyberactivity is measuring the amount of programming resources an attack requires—like malware designed to leap across air gaps. “If you see a huge amount of organization and programming going into an attack, that’s a good indicator that there’s a government involved.”

The U.S. and Europe remain extremely vulnerable to infrastructure attacks—especially as so much of these developed economies’ vital infrastructure is now electronic, from financial systems to social networks. One small example: In late April, a fleet of American Airlines Boeing 737s was temporarily grounded after an iPad application known as an “electronic flight bag” used by pilots for preflight checks crashed. The iPad app replaced 13 pounds of paper manuals—but when it went down, so did the entire fleet.

More worrying, though still hypothetical: The U.S. Government Accountability Office issued an official warning in April that “modern aircraft’s interconnectedness can potentially provide unauthorized remote access to aircraft avionics systems” and that an aircraft’s Wi-Fi access could be exploited by hackers. When security researcher Chris Roberts joked on Twitter about how easy it would be to “start playing with the EICAS”—Engine-Indicating and Crew-Alerting System—he was bumped off a flight. Boeing issued a statement saying that “no changes to the flight plans loaded into the airplane systems can take place without pilot review and approval.”

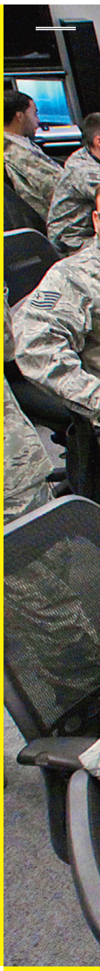
Other infrastructure is just as unprotected. A recent survey by the energy industry consultants Black & Veatch revealed that only 32 percent of U.S. electric utility companies had integrated security systems with the “proper segmentation, monitoring and redundancies needed for cyberthreat protection.”

In February, President Barack Obama set up a new Cyber Threat Intelligence Integration Center, described as “a national intelligence center focused on connecting the dots regarding malicious foreign cyberthreats to the nation.” Defense Secretary Carter made a trip to the heart of Silicon Valley, this month to help improve relationships with tech companies after damaging revelations by former National Security Agency contractor Edward Snowden about digital surveillance. “This threat affects us all,” Carter told the assembled techies. “There are also really great opportunities to be seized through a new level of partnership between the Pentagon and Silicon Valley.”

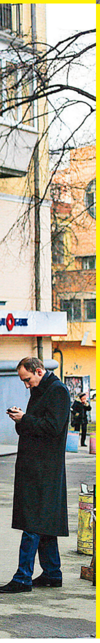
Behind the scenes, American spy agencies are also busy fighting a secret war against cyberenemies. Snowden—now in hiding in Russia—publicly revealed the massive scale of data mining by U.S. intelligence agencies, often in apparent violation of protections for U.S. citizens’ privacy. But a recent report by Kaspersky Labs suggests that the U.S. is no slouch in the hacking department either. A hacking collective that Kaspersky’s team dubbed Equation Group—sponsored, it coyly says, “by a nation-state with nearly unlimited resources”—has for the past 14 years apparently been busy planting top-flight spyware around the world, including a keystroke-logging program called Grok and a protective encryption system known as GrayFish.

The top targets? Iran and Russia, followed by Pakistan, China and India. The malware has targeted financial, government, diplomatic, aerospace and telecommunications networks, as well as research institutions and universities. According to Kaspersky’s engineers, the Equation Group designed “the world’s most mysterious malware warhead” as well as “a secret storage vault that survived military-grade disk wiping and reformatting, making sensitive data stolen from victims available even after reformatting the drive and reinstalling the operating system.”

Thanks to its vast resources, the U.S. may well be able to stay one step ahead of its cyberenemies. But the problem with this new battlefield is that none of the potential combatants know the rules—and, even more dangerous, no one can be certain of who the combatants are. “It is not always possible to distinguish between cyberespionage, cyber covert action and, most importantly, preparation for cybersabotage or war,” says Klimburg. “Serious misunderstandings are preprogrammed.... The consequences of misidentifying the motive of the attacker could



LEFT: VINCENT MUNDY/BLOOMBERG/GETTY; RIGHT: RICK WILKING/REUTERS



WAR ROOM: In February, President Obama created a new Cyber Threat Intelligence Integration Center to coordinate the work of numerous U.S. military and intelligence agencies that have their own cybersecurity operations.

LEFT: VINCENT MUNDY/BLOOMBERG/GETTY; RIGHT: RICK WILKING/REUTERS

be, in diplomatic-speak, 'inadvertent escalation'—or accidental cyberwar."

Richard Clarke, head of cybersecurity and counterterrorism coordination in the George W. Bush administration, has warned of the dangers of a "false flag" cyberattack designed to create tension between the U.S. and, for instance, China and launched by a hidden third party.

Some academics have proposed "cybermilitary exercises" between the United States and Russia as a vehicle for trust building. Others suggest establishing "rules of the road"—a kind of informal agreement for cyberspace that outlines what is a legitimate target for espionage purposes, with an agreement not to target supercritical infrastructure such as power grids with cyberespionage attacks.

"IN KIEV THEY MADE THE BANK'S ATMS SPEW OUT MONEY, WHICH WAS COLLECTED BY PEOPLE WALKING BY."

But even if Beijing could be persuaded to come on board, the current geopolitical tension between Washington and Moscow is hardly conducive to gentleman's agreements. Russian President Vladimir Putin has characterized the Internet as a "CIA invention" and this month ordered the FSB to "cleanse the Russian Internet" by forcing all Internet providers to keep their servers in Russia—another turn of the screw in the Kremlin's long-term plan to create a separate Russian Internet, a project to which Putin has pledged some $100 million since 2012. And during the Sochi Olympics in February 2014, the FSB deployed aggressive cyberspying tools designed to infect foreign visitors' computers and cellphones with spyware through Wi-Fi networks and cellphone towers.

It is unlikely that such a regime would shy away from using every cyberweapon at its disposal. It's equally unlikely that, faced with a barrage of what White House spokeswoman Jan Psaki described as "hundreds of cyberattacks a day," the U.S. will cease and desist from developing some of the world's most sophisticated cyberweapons in retaliation. The cyber arms race is on. N