# Cyberwar Ignites a New Arms Race

Dozens of countries amass cyberweapons, reconfigure militaries to meet threat

Defensive cyber operations at Petersen Air Force Base in Colorado Springs, Colo. ENLARGE

Defensive cyber operations at Petersen Air Force Base in Colorado Springs, Colo. PHOTO: RICK WILKING/REUTERS

By DAMIAN PALETTA, DANNY YADRON and JENNIFER VALENTINO-DEVRIES

Oct. 11, 2015 8:52 p.m. ET

33 COMMENTS

Countries toiled for years and spent billions of dollars to build elaborate facilities that would allow them to join the exclusive club of nations that possessed nuclear weapons.

Getting into the cyberweapon club is easier, cheaper and available to almost anyone with cash and a computer.

A series of successful computer attacks carried out by the U.S. and others has kicked off a frantic and destabilizing digital arms race, with dozens of countries amassing stockpiles of malicious code. The programs range from the most elementary, such as typo-ridden emails asking for a password, to software that takes orders from a rotating list of Twitter handles.

The proliferation of these weapons has spread so widely that the U.S. and China—longtime cyber adversaries—brokered a limited agreement last month not to conduct certain types of cyberattacks against each other, such as intrusions that steal corporate information and then pass it along to domestic companies. Cyberattacks that steal government secrets, however, remain fair game.

This comes after other countries have begun to amass cyberweaponry on an unprecedented scale. Pakistan and India, two nuclear-armed rivals, regularly hack each other's companies and governments, security researchers said. Estonia and Belarus are racing to build defensive shields to counter Russia. Denmark and the Netherlands have begun programs to develop offensive computer weapons, as have Argentina and France.

In total, at least 29 countries have formal military or intelligence units dedicated to offensive hacking efforts, according to a Wall Street Journal compilation of government records and interviews with U.S. and foreign officials. Some 50 countries have bought off-the-shelf hacking software that can be used for domestic and international surveillance. The U.S. has among the most-advanced operations.

In the nuclear arms race, “the acronym was MAD—mutually assured destruction—which kept everything nice and tidy,” said Matthijs Veenendaal, a researcher at the NATO Cooperative Cyber Defence Centre of Excellence, a research group in Estonia. “Here you have the same acronym, but it’s ‘mutually assured doubt,’ because you can never be sure what the attack will be.”

Governments have used computer attacks to mine and steal information, erase computers, disable bank networks and—in one extreme case—destroy nuclear centrifuges.

Nation states have also looked into using cyberweapons to knock out electrical grids, disable domestic airline networks, jam Internet connectivity, erase money from bank accounts and confuse radar systems, experts believe.

Large conventional militaries and nuclear forces are ill-suited to this new kind of warfare, which evens the playing field between big and small countries. Cyberattacks are hard to stop and sometimes impossible to trace. The West, as a result, has been forced to start reconfiguring its militaries to better meet the threat.

CATALOGING THE WORLD’S CYBERFORCES

ENLARGE

AGENCE FRANCE-PRESSE/GETTY IMAGES

More than 60 countries are developing cyberweapons. A guide to nations’ programs and capabilities.

Access to cyberweapons, according to U.S. and foreign officials and security researchers, is far more widespread than access to nuclear weapons was at the height of the nuclear arms race, a result of inexpensive technology and the power of distributed computing.

More than two dozen countries have accumulated advanced cyberweapons in the past decade. Some Defense Department officials compare the current moment to the lull between the World Wars when militaries realized the potential of armed planes.

“It’s not like developing an air force,” in terms of cost and expertise, said Michael Schmitt, a professor at the U.S. Naval War College and part of an international group studying how international law relates to cyberwarfare. “You don’t need to have your own cyberforce to have a very robust and very scary offensive capability.”

For example, hackers aligned with the Syrian government have spied into the computers of rebel militias, stolen tactical information and then used the stolen intelligence in the ongoing and bloody battle, according to several researchers, including FireEye Inc.

Most cyberattacks linked to the U.S. and foreign governments in recent years involve cyberspying—breaking into a computer network and stealing data. More-aggressive covert weapons go further, either erasing computer records or destroying physical property.

“With some countries, we’re comfortable with knowing what their capabilities are, but with other countries we’re still lost,” said Andre McGregor, a former cyber special agent at the Federal Bureau of Investigation and now the director of security at Tanium Inc., a Silicon Valley cybersecurity startup. “We don’t have the visibility into their toolset.”

The Military Balance, a widely read annual assessment of global military powers published by the International Institute for Strategic Studies in London, tallies tanks, battalions and aircraft carriers. When it comes to national cyberforces it says “capabilities are not assessed quantitatively.”

In the U.S., the National Security Agency, Central Intelligence Agency, FBI and others all play roles in combing through intelligence.

U.S. officials say their biggest concerns are the cyberweapons held by the Chinese, Russians, Iranians and North Koreans, countries that have deployed advanced attacks that either dug inside U.S. government networks or targeted top U.S. companies. Even Israel, a U.S. ally, was linked to hacking tools found on the computers of European hotels used for America’s diplomatic talks with Iran, according to the analysis of the spyware by a top cybersecurity firm. Israeli officials have denied spying on the U.S.

Cyberarmies tend to be integrated with a country’s military, its intelligence services, or both, as is the case in China and the U.S.

In China, hackers are famous for the relatively low-tech tactic of “phishing”—sending a flood of disguised emails to trick corporate employees and government bureaucrats to letting them into their networks.

The U.S. suspects that is how they penetrated the Office of Personnel Management, using a phishing email to breach an OPM contractor and then crack the agency’s network. The records of more than 21 million people were exposed in the 2014 and 2015 data breach, disclosed this summer. China has said it wasn’t involved.

China’s army has divisions devoted to cyberattacks, and recent evidence shows links between the country’s military and hackers who appear to be pressing the country’s interests abroad.

“They used to be snap and grab—get in and dump everything they can,” said Tommy Stiansen, co-founder and chief technology officer at Norse Corp., a California cybersecurity firm that tracks nation-state activity. “Now they trickle out the information, stay hidden in the system. We’ve even seen Chinese actors patch and repair networks once they’ve broken in.”

China opposes the militarization of cyberspace or a cyberarms race, said Zhu Haiquan, a spokesman for the Chinese Embassy in Washington, adding China “firmly opposes and combats all forms of cyberattacks in accordance with law.”

Choosy in targets

Russian hackers have targeted diplomatic and political data, burrowing inside unclassified networks at the Pentagon, State Department and White House, also using emails laced with malware, according to security researchers and U.S. officials.

They have stolen President Barack Obama’s daily schedule and diplomatic correspondence sent across the State Department’s unclassified network, according to people briefed on the investigation. A Russian government spokesman in April denied Russia’s involvement.

“Russia has never waged cyberwarfare against anyone,” Andrey Akulchev, a spokesman for the Russian Embassy in Washington, said in a written statement Friday. “Russia believes that the cybersphere should be used exclusively for peaceful purposes.”

Russia’s top hackers tend to be choosier in their targets, tailoring email attacks to those they believe might unwittingly open links or attachments.

“They are sitting there trying to think through ‘how do I really want to compromise this target?’ ” said Laura Galante, director of threat intelligence at FireEye, a Silicon Valley cybersecurity company that works closely with Washington. “The Chinese just want a foothold into the target. Russian theft is very personal.”

U.S. spies and security researchers say Russia is particularly skilled at developing hacking tools. Some malicious software linked to Russia by security researchers has a feature meant to help it target computers on classified government networks usually not connected to the Internet.

The virus does this by jumping onto USB thumb drives connected to targeted computers, in the hopes that the user—such as U.S. military personnel—will then plug that USB drive into a computer on the classified network.

ENLARGE

Russian hackers also make efforts to hide stolen data in normal network traffic. In one example, a piece of malware hides its communications in consumer Web services to fool cybersecurity defenses. The code downloads its instructions from a set of Twitter accounts. It then exports data to commercial storage services. This tactic is effective because corporate cybersecurity systems often don’t block traffic to and from these sites.

Iranian hackers have gone beyond stealing information; they have allegedly used cyberweapons at least twice to destroy computers.

Government investigators believe Iranian hackers implanted the Shamoon virus on computers at Saudi Arabia’s Saudi Aramco, the world’s largest energy firm, in 2012. The Aramco attack erased 75% of the company’s computers and replaced screen images with burning American flags. The attack didn’t affect oil production, but it rattled the company, and security officials, as it revealed the extent of Iran’s cybercapabilities. A spokesman for Aramco didn’t respond to a request for comment.

The move was at least partly in retaliation for the alleged U.S.-Israeli attack on Iran discovered in 2010 that deployed the Stuxnet computer worm to destroy Iranian nuclear centrifuges—considered to be the most successful and advanced cyberattack ever. The U.S. and Israel haven’t confirmed or denied involvement with Stuxnet.

Director of National Intelligence James R. Clapper has said that Iran used malware to destroy computers last year at Las Vegas Sands Corp., a casino company run by Sheldon Adelson, a major critic of the Iranian government. A Sands spokesman declined to comment.

Adm. Michael Rogers, center, director of the National Security Agency and commander of the U.S. Cyber Command, confers with Deputy Defense Secretary Robert Work ahead of testifying before the Senate Armed Services Committee in September. ENLARGE

Adm. Michael Rogers, center, director of the National Security Agency and commander of the U.S. Cyber Command, confers with Deputy Defense Secretary Robert Work ahead of testifying before the Senate Armed Services Committee in September. PHOTO: WIN MCNAMEE/GETTY IMAGES

Defense officials have also said Iranian hackers have temporarily overwhelmed the websites of numerous U.S. banks, in an annoying but relatively pedestrian technique known as a “denial of service” attack. The attack was allegedly in response to a YouTube video depicting the Prophet Muhammad. Some U.S. officials suspected it was retaliation for sanctions and the Stuxnet attack.

In 2012, Iran’s Supreme Leader Ayatollah Ali Khamenei publicly announced the creation of the Supreme Council of Cyberspace charged to oversee the defense of Iran’s computer networks and develop “new ways of infiltrating or attacking the computer networks of its enemies.”

National Security Agency Director Adm. Michael Rogers said Iranian cyberattacks have slowed since nuclear talks intensified last year, but that Tehran appears “fully committed” to using cyberattacks as part of its national strategy.

A spokesman for the Iranian government didn’t respond to request for comment.

## Sony hack

U.S. officials accused North Korea of destroying computer files and records at Sony Corp.’s Hollywood film unit in 2014, allegedly in retaliation for “The Interview,” a satirical movie about assassins of North Korean leader Kim Jong Un. The breach was considered one of the most successful nation-state attacks. North Korea successfully implanted malware on Sony computers, which allowed them to both steal and destroy company records, the FBI alleged.

South Korea has also accused North Korea of trying to hack a nuclear reactor, television networks and at least one bank.

“Cybercapability, especially offensive cybercapability, is a relatively inexpensive method that a country can exploit to ‘hit above its weight class,’ which North Korea is fully aware of and is attempting to leverage,” said Steve Sin, a former U.S. Army counterintelligence officer who now researches unconventional weapons and technology.

Defense contractor Northrop Grumman Corp., meanwhile, has advertised for a “cyber operations planner” to “facilitate” offensive computer attacks with the South Korean and U.S. governments, according to a job posting it listed online.

A Northrop spokesman said the customer determines the scope of work performed.

A spokesman for North Korea couldn’t be reached for comment. The country hasn’t commented publicly on cyberprograms.

Many cybersecurity experts, however, consider the U.S. government to have the most advanced operations. When Kaspersky Lab ZAO, a Russian cybersecurity company, this year released a report on a group it called the Equation Group—which U.S. officials confirmed was a thinly veiled reference to the NSA—it referred to the operatives as the “crown creator of cyberespionage.”

Former National Security Agency contractor Edward Snowden leaked documents that showed the NSA had implanted malware on tens of thousands of foreign computers. That allowed the U.S. government secret access to data and, potentially, the industrial control systems behind power plants and pipelines. The Pentagon’s U.S. Cyber Command didn’t respond to a request for comment.

In some instances, Kaspersky found, the NSA was able to burrow so deeply into computers that it infected the code that controls how a hard drive spins. So-called firmware isn’t scanned by computer defenses.

“We, too, practice cyberespionage, and, in a public forum, I’m not going to say how successful we are, but we’re not bad,” Mr. Clapper, the Director of National Intelligence, told a Senate panel in September.

U.S. Cyber Command now has nine “National Mission Teams” with plans to build four more. These each comprise 60 military personnel that will “conduct full-spectrum cyberspace operations to provide cyber options to senior policy makers in response to attacks against our nation,” a Pentagon spokesperson said.

The Navy, Army, and Air Force will each build four teams, with the Marines building a single unit. Each will have a “separate mission with a specific focus area,” though these have so far remained secret.

Air Force Chief of Staff Gen. Mark A. Welsh III told a group of reporters in April that he wanted to see the military develop “blunt force trauma” powers with their cyberweapons. He gave examples of computer codes that could “make an enemy air defense system go completely blank” or have an enemy’s “radar show a thousand false targets that all look real.” He didn’t say the military had finished designing such powers.

Defense Secretary Ash Carter has made the development of new cyberweapons a priority, although the policy seems in flux after questions were raised by the Pentagon’s inspector general.

This activity has prompted other countries to join the digital buildup.

In 2014, the Netherlands announced it would begin training its own Internet troops through a domestic cybersecurity company, called Fox-IT. The head of the Dutch armed forces, Major Gen. Tom Middendorp, said in a symposium the group should be prepared to carry out attacks, not just block them, according to a Dutch media report. The Netherlands’ military strategy, laid out in various documents, refers to hacking as a “force multiplier.” A Dutch military spokesman confirmed the efforts but declined to make Gen. Middendorp available for an interview.

In 2013, Denmark’s Defense Ministry began allocating about $10 million a year for “computer network operations,” which include “defensive and offensive military operations,” according to government budget documents. That amount is just 0.24% of the Danish defense budget, reflecting the tiny barrier of entry.

Countries unable to develop their own weapons can buy off-the-shelf systems from private parties. Earlier this year, an attack and document leak on the Italian firm Hacking Team revealed the company had sold its surveillance tools to dozens of countries, including Sudan, Egypt, Ethiopia and Azerbaijan.

Hacking Team touted its product as “the hacking suite for governmental interception,” and computer security researchers who studied its program said it took advantage of holes in popular software to get onto opponents’ computers and mobile devices. The FBI is among the groups listed as clients of Hacking Team. An FBI spokesman said it didn’t comment on specific tools or techniques.

Most of these countries use surveillance software on domestic enemies or insurgent groups, according to officials with numerous countries and researchers.

States aren’t the only players. About 30 Arabic-fluent hackers in the Palestinian territories, Egypt and Turkey are building their own tools to hit targets in Egypt, Israel and the U.S., according to researchers at Kaspersky Lab.

And in August, the U.S. used a drone to kill Islamic State hacker Junaid Hussain in Raqqa, Syria, showing the extent to which digital warfare has upset the balance of power on the modern battlefield.

The British citizen had used inexpensive tools to hack more than 1,000 U.S. military personnel and published personal and financial details online for others to exploit. He helped sharpen the terror group’s defense against Western surveillance and built hacking tools to penetrate computer systems, according to people familiar with the matter.

National-security and cyberweapon experts are watching the growing digital arms stockpile nervously, worried that one-off attacks could eventually turn messier, particularly given how little is known about what each country is capable of doing.

“What we can do, we can expect done back to us,” said Howard Schmidt, who was the White House’s cybersecurity coordinator until 2012. The U.S. is thinking, “Yeah, I don’t want to pull that trigger because it’s going to be more than a single shot that goes off.”

Write to Damian Paletta at damian.paletta@wsj.com, Danny Yadron at danny.yadron@wsj.com and Jennifer Valentino-DeVries at Jennifer.Valentino-DeVries@wsj.com