THE WALL STREET JOURNAL.

The Wall Street Journal. – 09.11.2015

By Margaret Coker and Paul Sonne

Ukraine: Cyberwar's Hottest Front

Ukraine gives glimpse of future conflicts where attackers combine computer and traditional assaults

Україна: передовий фронт кібервійни

Україна дає уявлення про конфлікти майбутнього, де агресори поєднують комп'ютерні та традиційні атаки

Напередодні президентських виборів в Україні ЦВК атакував тіньовий промосковський колектив хакерів "КіберБеркут", згадують автори статті. Зрештою атака не змогла пустити голосування під укіс. Українські комп'ютерники мобілізувалися і встигли відновити роботу системи до виборів. Але це вторгнення стало для України початком нової епохи і показало, як геополітична конфронтація з Росією може призвести до змови кіберворогів, спрямовану на те, щоб підточити авторитет влади, яка намагається порвати з Кремлем, і поставити їх у незручне становище, - вважають автори. Україна дає уявлення про гібридні війни, до яких зараз в терміновому порядку готуються західні воєначальники. Про битви, у яких традиційні наземні війська діють спільно з солдатами кіберармії, щоб послабити і розбити супротивника. Ситуація також показує, з якими труднощами стикається країна, коли їй необхідно викрити більш сильного кіберворога і захиститися від нього ", - вказують автори.

http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671

A woman votes in Kiev in May 2014. A cyberattack ahead of Ukraine's 2014 presidential election threatened to derail the vote. Photo: Dan Kitwood/Getty Images

KIEV, Ukraine—Three days before Ukraine's presidential vote last year, employees at the national election commission arrived at work to find their dowdy Soviet-era headquarters transformed into the front line of one of the world's hottest ongoing cyberwars.

The night before, while the agency's employees slept, a shadowy pro-Moscow hacking collective called CyberBerkut attacked the premises. Its stated goal: To cripple the online system for distributing results and voter turnout throughout election day. Software was destroyed. Hard drives were fried. Router settings were undone. Even the main backup was ruined.

The carnage stunned computer specialists the next morning. "It was like taking a cold shower," said Victor Zhora, director of the Ukrainian IT firm Infosafe, which helped set up the network for the elections. "It really was the first strike in the cyberwar."

In just 72 hours, Ukraine would head to the polls in an election crucial to cementing the legitimacy of a new pro-Western government, desperate for a mandate as war exploded in the country's east. If the commission didn't offer its usual real-time online results, doubts about the vote's legitimacy would further fracture an already divided nation.

The attack ultimately failed to derail the vote. Ukrainian computer specialists mobilized to restore operations in time for the elections. But the intrusion heralded a new era in Ukraine that showed how geopolitical confrontation with Russia could give rise to a nebulous new cabal of cyberfoes, bent on undermining and embarrassing authorities trying to break with the Kremlin.

In the last two years, cyberattacks have hit Ukraine's Ministry of Foreign Affairs, Ministry of Defense and the presidential administration. Military communications lines and secure databases at times were compromised, according to Ukrainian presidential and security officials. A steady flow of hacked government documents have appeared on the CyberBerkut website.

Ukraine offers a glimpse into the type of hybrid warfare that Western military officials are urgently preparing for: battles in which traditional land forces dovetail with cyberattackers to

degrade and defeat an enemy. It also illustrates the difficulties that nations face in identifying and defending against a more powerful cyberfoe.

Ukrainian leaders are lacking in capabilities needed to mount a response to the electronic attacks. North Atlantic Treaty Organization members last year agreed to fund and build a new cyberdefense command center for Kiev, but legislative and bureaucratic delays have stalled the project. Ukraine is still working on passing a new law designed to step up its digital defenses.

Officials in Kiev are united in their accusations about who is orchestrating or commissioning the hundreds of cyberattacks they have tallied: Russia. They cite Russia's military doctrine that describes cyberweaponry as a key pillar of the country's armed forces and the adoption of "enhanced and nonmilitary measures" to achieve military goals. The officials, however, didn't offer any smoking gun linking the attacks to Moscow's security services.

"We consider that there is only one country in the world that would benefit from these attacks, and this is Russia," said Vitaliy Naida, Ukraine's head of counterintelligence.

Kremlin spokesman Dmitry Peskov denied the accusations, calling them "absurd" and noting that Russian computers are also regularly attacked by hackers. The Kremlin has denied that Russian military personnel played a role in occupying parts of east Ukraine and in backing rebels there.

CyberBerkut posted its claim of responsibility for the election commission hack on its website a day after the attack. The group presents itself as an independent Ukrainian organization. It didn't respond to requests sent via its website for comment about allegations that it works on behalf of Russia. It has never revealed the names of its members.

U.S. spies and security researchers say Russia is particularly skilled at developing hacking tools. They blame Russia for breaking into President Barack Obama's email and infiltrating unclassified servers at the Pentagon and State Department. Russia has denied the accusations.

Ukraine has a plethora of criminal hackers, who are pursued by the Federal Bureau of Investigation and Ukraine's recently launched cyberpolice for their alleged role in bank fraud, among other crimes, but the Ukrainian government hasn't recruited them for cyber counterattacks or defense against Russia, according to Mr. Naida.

When Russia seized Crimea and backed the uprising in the Donbas region of eastern Ukraine in early 2014, cyberinvaders had easy access to the country's largely unguarded electronic frontiers.

The country was particularly vulnerable to cyberattacks and espionage, given its high reliance on Russian technology, ranging from the telecommunications backbone to the antivirus software that was running on many government computers. At the same time, Russia loyalists riddled the ranks of the security service, challenging any attempt to put up defenses.

Ukrainian government officials, including those in the security services and military, habitually conducted official business via personal email addresses hosted by Russian-language email platforms with servers based in Russia, according to Mr. Naida, the counterintelligence chief.

Infecting Ukraine

Ukraine officials blame Moscow for a series of cyberattacks both before and after the country's 2014 presidential elections, allegations that Russia denies. Here are some of the alleged actions taken by hackers:

Ukraine vulnerabilities

High reliance on Russian technology, from the telecommunications backbone to the antivirus software running on many government computers.

Russia loyalists riddle the ranks of the security service, challenging any attempt to put up defenses.

ENLARGE

Even today, more than half of Ukrainian government computers operate pirated software, lacking proper security updates, and many also use Russian antivirus software, according to Dmytro Shymkiv, the deputy head of the presidential administration and a former Microsoft executive in Ukraine.

These vulnerabilities mean that since last year hundreds of government computers have been compromised by malware designed for espionage, according to Ukrainian officials and computer experts who have investigated the attacks.

Computer engineers say most of those infections trace back to four unique computer virus families that have developed independently of one another but share certain basic characteristics. The virus creators typed in Cyrillic; they worked in a time zone that encompasses Moscow and Kiev; and they included sophisticated coding likely requiring full-time efforts, indicating sponsorship by a nation-state.

"These are very customized," said Alan Neville, from the computer security response department at Symantec Corp. , a global computer security company. "No one is going to take time to develop a tool unless they are under orders to do so or have a contract to do so."

One computer virus strain targeting the Ukrainian government was malware first used in a Russian Ponzi scheme in 2012, which hackers have retooled for cyberespionage, according to security company ESET, which analyzed the malware for its Ukrainian clients.

Another separate strain is an evolved version of malware that attacked U.S. military's Central Command computer servers in 2008, a virus that U.S. officials believe was developed by Russian state agencies.

Russia has denied this allegation.

The enhanced virus—dubbed Turla, or Snake in English—infected Ukrainian diplomatic computers, according to computer experts familiar with the situation, as an intrusive tool to steal sensitive data.

Primary targets were Ukrainian embassies in Europe, including those in Belgium and France, these people said. Through the summer of 2014, Ukraine's diplomats lobbied Western capitals to take a stronger stance against Moscow's aggression.

"Turla started to appear in Ukraine starting with the beginning of the conflict early last year," says Alex Gostev, chief security expert at Moscow-based Kaspersky Lab.

Dmytro Shevchenko, a spokesman for Ukraine's Ministry of Foreign Affairs, said cyberattacks against the ministry's institutions took place "steadily, all the time" during 2014, aimed primarily at espionage. He didn't detail the type of viruses.

Mr. Naida said that infections haven't penetrated the ministry's classified servers.

Western officials said the Foreign Ministry breach was inconvenient, but that it didn't adversely affect Ukraine's diplomatic goals.

The ministry's attempt to parry the infection last year was to delete work email identities of its diplomats and assign them new email addresses on new servers. Ukraine's government computer specialists also tackled the infection.

Within the armed forces, cyberattackers have targeted security units battling pro-Russian rebels in eastern Ukraine, including a classified computer network at the military headquarters in Kramatorsk, according to Mr. Naida. "The aim was to kill all the information, to destroy all the information on those computers" to cripple intelligence-gathering and decision-making by commanders, he said. He declined to give specifics about the damage caused by the attack.

Political upheaval

By the time of the May 2014 election, Ukraine's new pro-Western leaders were desperate to cement their authority. Pro-Western demonstrators in Kiev had forced President Viktor

Yanukovych to step down. Russia was covertly supporting a territorial grab by rebels in the east, and the new acting president lacked a mandate to lead Ukraine's troops.

Ukraine itself was divided. Russian propaganda regularly assailed the acting authorities in Kiev as an illegitimate "junta" installed by the West. A large swath of Russian-speaking Ukrainians in the east sympathized.

Amid this political friction, election commission officials finished the routine preparations for a national vote. They commissioned a commercial computer company to help set up the necessary IT infrastructure to upload preliminary results and voter turnout numbers.

Three days before the Sunday election, CyberBerkut issued a statement denouncing the vote. "The anti-people junta is trying to legalize itself by organizing this show, directed by the West," the group said. "We will not allow it!"

At around 3 a.m. Thursday, the group launched its attack, spending hours rooting through the network and destroying data, according to Ukrainian officials and computer experts.

When the workday started, the agency's staff discovered the damage. They no longer had the ability to provide a real-time tally of the voting results. Although Ukrainian voters would still be able to cast their paper ballots, a lack of immediate official results could hurt the election's legitimacy.

With just over 48 hours until the start of the election, Ukraine's cyberspecialists, including those in the security service, camped out at the election agency headquarters, some fueled by Red Bull to keep them awake, as they tried to rebuild the system. "Our people didn't sleep for five days," Mr. Zhora said.

The details of the events in the days after the attack come from interviews with four Ukrainian security and election officials and computer experts involved in the investigation.

The specialists immediately had a lucky break: The original team that had set up the network had created a second backup of the system, disconnected from the Internet, giving them a timesaving head start.

CyberBerkut taunted the commission. It released a string of documents from the election agency's network, including photos of the election commissioner's bathroom renovation, pictures of his and his wife's passports and emails sent by Western officials to Ukrainian election organizers.

"Before there were little things—[distributed denial of service] attacks and viruses. But this was a serious, preplanned attack," said Valeriy Striganov, the head IT operator at the election commission.

The attackers published online what they called a "report on the hack," which included a detailed map of the Central Election Commission's computer network. The group claimed to have penetrated the system using a zero-day vulnerability—an unknown hole in a software application—in the network's Cisco firewall.

Ukrainian authorities later passed the information to Cisco Systems Inc. The U.S.-based company said it found no vulnerability in its product.

At election headquarters, the team scrambled to bolster the system's defenses against any fresh attack. They tightened restrictions over who could access the election results data. They also cut off Internet access to computers at commission headquarters.

By the time the sun rose on May 25, the downed system had come back to life, and Ukrainians headed to the polls. But a fresh assault had already started.

Hackers bombed the Central Election Commission website with a distributed denial-of-service attack, attempting to bring the system down again by causing it to seize up from the volume and intensity of computer messages.

The site stayed up, thanks to the stronger defenses.

As Sunday progressed, preliminary results indicated that Petro Poroshenko, a chocolate tycoon and former foreign minister, was on pace to win a majority. Exit polls also suggested a poor showing by far-right candidates, despite Russian state media warning of a fascist takeover in Ukraine.

Then, one of the far-right candidates appeared to get a strange boost. A hoax chart depicting a victory for extreme-right candidate Dmytro Yarosh appeared online. The Central Election Commission seemed to be hosting the file.

Soon, Russia's most popular state news program was showing the chart on air. Hackers appear to have placed the file on the server that usually hosts the election commission website, and then circulated that Web address, according to people familiar with the incident, who said the image wasn't accessible to the general public from the main home page at the time.

In a statement, CyberBerkut suggested it wasn't responsible for the faked results, saying those looking for answers should ask Ukraine's election commissioner. No other claim of responsibility has been made.

The faked results were almost immediately debunked, and Russian television posted authentic tallies from the election commission. The day ended with Mr. Poroshenko winning 55% of the vote.

The head of the Special Communications Service at the time characterized the election attack as an urgent warning of Ukraine's vulnerabilities. It was one of the few sizable attacks publicized by Ukrainian authorities, in part because specialists managed to salvage the system.

Attacks that cause irreparable damage tend to go unrevealed. "Very often when there is a real penetration you will never hear [about it], because it's never disclosed," says Mr. Shymkiv. "At the same time, when somebody defends it, you will hear the stories."

Write to Margaret Coker at margaret.coker@wsj.com and Paul Sonne at paul.sonne@wsj.com