Global Cyber Bi-Weekly Report by INSS August 1 2018

Editor-in-chief: Gabi Siboni, **Editor:** Hadas Klein, Gal Perl Finkel

Contributors: Simon Tsipis, Ido Sivan, Anna Danilova, , Bryan McCarthy

ISRAEL

Israel is under massive Chinese, Russian cyber espionage attack

A few months ago, "Ophir," a senior official in the Shin Bet's counter-espionage division with a rich intelligence background who had turned into a private cybersecurity expert, was called back to duty. He and a team of experts were asked by Israel's government intelligence and information protection agencies to examine the security of some of Israel's main computer systems. A few systems were defined as "strategic," others of lesser importance. "We believe Israel is under a multi-frontal attack, a significant threat to our national security. Some of the spying is classic, like it used to be: living agents recruited for personal gain or ideology. We know how to deal with those. But some attacks are being carried out by other means, less visible and clear," said Ophir. Iran is the immediate suspect in the attack. The international boycott against the Islamic Republic forced Iran to build its own communications and encryption systems. To that end, Iran set up an impressive network of cyber institutions and engineers and greatly improved its capabilities of stealing technology, hacking into databases, and planting viruses. For years now, Israel's intelligence community has witnessed many attacks on Israeli computers by Iranian intelligence. The question is, of course, what it does not see, where the breaches in the barriers are, and what roles do Hamas and Hezbollah play. "Today, the Shin Bet is facing more significant challenges," says a former Shin Bet's counter-espionage division commander. These challenges are called China and Russia.

https://bit.ly/2Khqqs2

Global success to safety and security system developed by Israeli start-up

The Israeli start-up company NowForce has developed a ground-breaking solution for the management of incidents and events in emergency and routine, first responder management, and real-time situational awareness for

the incident managers. It is a flexible command and control system available either as an on-site installation or a cloud-based service, with simple and rapid installation. NowForce was founded in 2008 by three entrepreneurs—Jonathan Bendheim, Fibro Israel's CEO; Assaf Shafran, an Israeli Air Force navigator; and Anshel Pfeffer, a former IDF Paratroop Battalion Commander. Their professional experience has been the basis for the development of the company's technology. Last year, NowForce was named one of the top ten Homeland Security Solution Providers by govCIO, along with corporations such as Boeing and Lockheed Martin. The company won the first prize at the iHLS Start-up Competition for Security and Homeland Security in July 2018, granting an investment prize by Arieli Capital and participation at the fifth cycle of iHLS Security Accelerator.

https://bit.ly/2NVjZgw

UNITED STATES

US cyber forces will be more aggressive in entering enemies networks

The new head of US Cyber Command spoke recently at the Aspen Security Forum. He articulated that the US cyber forces will be more aggressive in entering enemies networks.

https://bit.ly/2mX626t

NSA chief forms group to counter Russian cyber threat

General Paul Nakasone has started a "Russia Small Group" to counter Russian cyber threats toward the United States. It is described as being more offensive than defensive and to have a focus on protecting US election infrastructure from Russian meddling during the upcoming 2018 mid-term elections.

https://bloom.bg/2LTbGos

Cybersecurity 202: Agencies struggling with basic cybersecurity despite Trump's pledge to prioritize it

According to the Washington Post, Senator Ron Wyden (D-Ore) is sounding the alarm that the executive branch is not practicing basic cyber hygiene. He claims the executive branch widely uses Adobe Flash, which is rife with security flaws. Not to be out done, the Government Accountability Office reported that the federal government has failed to implement hundreds of cyber defense recommendations. The NSA also has issues as of late. The agencies internal watchdog says employees are not following proper cybersecurity controls and best practices. On top of this, the NSA have many "inaccurate or incomplete" security plans.

https://wapo.st/2vjaz75

EUROPE

Only 7 percent of UK firms regularly train employees to spot phishing emails

As many as 54 percent of organizations in the United Kingdom have reported an increase in email-based phishing attacks launched by cybercriminals, with such attacks being launched across the entire organizational hierarchy from the C-suite, the finance department, HR staff members, to even trusted third-party vendors. This could be a direct result of the lack of training imparted to employees on how to spot cyberattacks. In the United Kingdom alone, only 7 percent of organizations continuously train employees, with 61 percent performing training just once a year. Globally, 11 percent of organizations continuously train employees on how to spot cyberattacks, 24 percent offer monthly training, and 52 percent perform training only quarterly or once a year.

https://bit.ly/2KdpViX

EU fines Google $5 billion over Android antitrust abuse

EU regulators have slapped Google with a record 4.34 billion Euro ($5 billion) antitrust fine for abusing the dominance of its Android mobile operating system, which is by far the most popular smartphone OS in the world. Google said in a statement that it would appeal the ruling, arguing against the European Union's view that its software is restrictive of fair competition.

European officials say Google's parent company, Alphabet Inc., has unfairly favored its own services by forcing smartphone makers to pre-install Google apps Chrome and Search in a bundle with its app store, Play.

https://bit.ly/2LRFNwh

UK consumers prefer security to convenience

UK consumers prioritize security over convenience far more than IT and business executives, according to a new study from CA Technologies. The firm commissioned analyst Frost & Sullivan to poll 990 consumers, 336 security professionals, and 324 business executives across ten countries, including nearly 600 respondents in Europe. It revealed that 83 percent of UK consumers prefer security over convenience when authenticating during transactions, while the figure is much lower for cybersecurity professionals at 60 percent, and business executives at 59 percent.

https://bit.ly/2M6oiW7

RUSSIA

Putin: Millions of cyberattacks on Russia were repelled during the World Cup

Russia's President Putin stated that during the World Cup in Russia, almost 25 million cyberattacks and other criminal influences on the country's information infrastructure were deterred. The president noted that 126 representatives of fifty-five special services and law enforcement agencies representing thirty-four countries participated in the security of the World Cup in Russia.

http://bit.ly/2NUzKVg

Putin to initiate US-Russian cybersecurity working group after US election fraud?

During their meeting at the G-20 Hamburg Summit, US president Donald Trump and Russian president Vladimir Putin had discussed the idea of a US-Russia cybersecurity working group, but Trump said that he doubted the

possibility of creating a working group between Moscow and Washington on information security. "The fact that President Putin and I discussed the creation of a working group on cybersecurity does not mean that I believe that this can happen. This cannot happen, but the agreement on a cease-fire in Syria—maybe it has already happened," wrote the American leader on Twitter.

http://bit.ly/2LViWNb

US military Cyber Command to organize special "Russian Department"

The commander of the US Cyber Command, Paul Nakasone, announced certain changes in the department under his control. According to Nakasone, the US Cyber Command will pay more attention to "Russian intervention." Speaking at a forum on cybersecurity in Colorado, Nakasone announced his personal decision to form a special group that would deal specifically with the "Russian issue."

http://bit.ly/2mPBjIv

Russia suspected of cyberattacks on nuclear facilities in the United States

US authorities have stated that hackers, working for foreign government, tried to disrupt at least twelve US power plants, including the Wolf Greek in Kansas. According to Bloomberg.com, the power plant's cybersecurity specialists assume that hackers were looking for weaknesses in the power grid. According to the publication, the main suspects in the commission of these attacks are Russian hackers, and the issue causes concern in the United States after Russian hackers, as the newspaper notes, have already undermined the operation of part of the power grid in Ukraine.

http://bit.ly/2uYlzqX

ASIA PACIFIC

Taiwan's emerging push for "cyber autonomy"

On May 11, Taiwan passed the Cybersecurity Management Law, Taiwan's first national cybersecurity law, which mandates cybersecurity requirements for Taiwan's government agencies and operators of critical infrastructures. The new law represents the latest initiative in the administration's push for cybersecurity under the policy "Cybersecurity is National Security." As part of this push, the administration is also working to develop Taiwan's indigenous cybersecurity industry through a policy of "cyber autonomy." The cyber threats to the island are substantial. Taiwan has been ranked as one of the top targets of advanced cyberattacks in the world that conduct cyber espionage against government agencies and corporate entities in Taiwan, mainly by state-initiated or state-sponsored advanced persistent threats, most of which can be traced to China. In April, the Department of Cybersecurity of Taiwan's executive branch of government revealed that China's "internet army" accounted for 288 successful attacks against Taiwan's government agencies in 2017. Last March, the director of Taiwan's National Security Agency admitted to the parliament that China's cyber penetration of Taiwan's networks is "worse than before."

https://bit.ly/2v5bvfO

Japan crafts new cybersecurity strategy for 2020 Tokyo Olympics

Japan's government crafted a new cybersecurity strategy as it steps up preparations for the Tokyo Olympic and Paralympic Games in 2020. It also decided to introduce a five-stage index to classify the severity of cyberattacks to help people understand the magnitude of threats and take necessary action. The five stages are based on how long it will take to recover, the size of the area affected as well as whether people were injured or forced to evacuate. The lowest level of zero indicates "no impact" while the highest level of four implies an "extremely grave impact." The strategy, pending approval from the cabinet, will be used as a cybersecurity guideline for the next three years. It also states the need to hold training and drills on the assumption of cyberattacks causing massive power outages and disrupting financial services. Yoshihide Suga, the chief cabinet secretary that leads the Cybersecurity Strategy Headquarters, said that "The likelihood of cyberattacks resulting in major economic losses is growing."

https://bit.ly/2vlSdlG

MIDDLE EAST

Saudi Arabia needs to invest in cybersecurity to secure its Saudi Vision 2030 plans

James Lyne, head of Research and Development at the SANS institute, has said that gaps between Saudi Vision 2030 plans, a knowledge-based economy, and the cybersecurity necessary to prevent attacks will damage Saudi's reputation in going forward. Attacks on Saudi Arabia are 6 to 8 percent higher than other Gulf countries. The cost associated with these attacks is 3 to 4 billion USD. According to Simone Vernacchia, a partner in Digital, Cybersecurity, Resilience, and Infrastructure for PWC Middle East, businesses in Saudi Arabia are not completely unprepared but are still not investing in the people and technology at the rate of the leading cybersecurity powers.

https://bit.ly/2OtHte6

Oman thwarted attacks on infrastructure

Oman thwarted 1.41 million cybersecurity attacks on government networks in 2017, according to the Information Technology Authority's Annual Report. The Annual report stated that Oman was one of the countries with the best practices for cybersecurity. The practices are good because of continued investment in cybersecurity. Oman also has continuous audits and checks, and is also actively comparing its capabilities to those of other countries. Oman also has ten partnerships with other countries so it can grow from their knowledge.

https://bit.ly/2mTL8oR

Egypt passes fake news law, curtailing internet freedoms

Any blog or website or social media account with five thousand followers can now be legally blocked by the Egyptian state. The bill, which was passed into law by the Egyptian parliament on July 16, is supposed to fight against fake news. However, it creates the Supreme Council for the Administration of the

Media, which allows the state to censor those who criticize the regime. The law, inspired by Abdel Fattah al-Sisi, is mainly designed to end criticism of the regime.

https://bit.ly/2NHJBNN

LATIN AMERICA

Mexican Central Bank says cyberattack cost 300 million pesos

Governor Alejandro Díaz de León, told the press that three banks, a broker, and a credit union had been targeted by cyberattacks. The governor also added that banks would be sanctioned if they did not comply with the security regulations set up by the central bank. The governor said it would take six months to determine if a second phase to the attack occurred. The attackers injected fraudulent payment instructions to affect the transactional accounts, which were attacked. It took two weeks for the funds to be reported as stolen.

https://bit.ly/2O04AvN

Chile's massive credit card information leak

A total of 55,106 credit cards were leaked in Chile last Saturday, and the vast majority of these cards are foreign. This comes after the information of 14,000 cards was published. State prosecutors have been called in for investigation. Santander Chile, a major bank in Chile, is investing 31 million USD in cybersecurity. Currently, the government of Chile is designing a bill that will create a cyber protection authority in the country. An International Monetary Fund report on the state of Chile's cybersecurity will be coming out later this year.

https://bit.ly/2OwxwfF

AFRICA

South Africa's growing cyber threats

Many South African based businesses and organizations are becoming increasingly exposed to threats and vulnerabilities of which they are not

aware. Companies lack appropriate design and implementation of cyber defense systems and the capability to detect and respond to IT security threats and breaches with appropriate levels of depth. Compliance with network infrastructure security directives and appropriately formulated cybersecurity rules designed to protect key industries like banking, energy, and technology from attacks is now of paramount importance in South Africa if serious cyber breaches are to be managed.

https://bit.ly/2LDPOOl

Hotels are hot targets for cyber criminals in Africa

The PwC Accounting firm has published a report about the common security breaches in hotels in the continent. Cyber lead for PwC Africa showed that regulators are coming down harder on companies, and South Africa will be no exception. The nation's Protection of Personal Information Act (PoPI) is expected to come into force next year, giving companies a year to comply. In between, the regulator is responding to privacy complaints and asking businesses to investigate and remediate.

https://bit.ly/2LSNjH6