Global Cyber Bi-Weekly Report by INSS June 1 2019

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

Contributors: Simon Tsipis, Gal Sapir, Robin Veldwijk, Thomas Abma

ISRAEL

Israeli banks under increasing threat from cyberattacks

Cyberattacks on Israel's banking system have increased considerably over the past two years. There are daily cyberattacks on Israeli banks, but so far none have caused major damage, according to the annual report by Supervisor of Banks Hedva Ber. The report found that 90 percent of the eighty high-ranking banking officials see cyber crimes as the most dangerous to their sector. More banks have moved their services online, in a positive move toward efficiency, which results in a higher risk of cyberattacks. Israeli banks have increased their investment in cybersecurity, setting up a joint body through which to share information and alerts. The banks are facing not only cyberattacks for financial gain but also may be targets of cyber terrorism.
https://bit.ly/2WcmuDW

Facebook busts Israel-based campaign to disrupt elections

Facebook has banned the Israeli company Archimedes Group, a Tel Aviv-based political consulting and lobbying firm that boasts of its social media skills and ability to "change reality," for running a campaign aimed at disrupting elections in various countries, and it has canceled dozens of accounts engaged in spreading disinformation. The ban contains 65 Israeli accounts, 161 pages, dozens of groups, and four Instagram accounts. Archimedes Group focused on Sub-Saharan African countries, parts of Southeast Asia, and Latin America, and the pages have racked up 2.8 million followers and hundreds of thousands of views. Gleicher, Facebook's head of cybersecurity policy, said Archimedes had spent some $800,000 on fake ads

and on created accounts posing as certain political candidates, smearing opponents, and presenting as local news organizations peddling supposedly leaked information. Their motives "may be commercial or political."
https://bit.ly/2Z0AI7X

HP teams with Deep Instinct on cybersecurity

HP Inc. (HPQ) has teamed with the New York and Tel Aviv-based cybersecurity company Deep Instinct to launch HP Sure Sense on its latest EliteBook and HP ZBook devices. HP says that HP Sure Sense is a standalone, self-managed solution that works on or offline, offering a simple, streamlined user-experience. HP Sure Sense is based on Deep Instinct's deep learning cybersecurity technology, and Deep Instinct was recently recognized in SE Labs' independent threat prevention evaluation test labs report for achieving a 100 percent prevention rate and zero false-positives when detecting and blocking known and unknown threats, including file-based and file-less attacks. "This is only the first step in what will be a long and strategic partnership between HP and Deep Instinct," said Deep Instinct co-founder and CEO Guy Caspi.
https://bit.ly/2Quqw4s

UNITED STATES

The Air Force names a new boss for "cyber effects"

Recent initiatives underway in the US Air Force regarding "information warfare, cyber electronic warfare and intelligence" have resulted in reorganization of staff, new leadership, and organizational development. Replacing Lt. Gen. VeraLinn Jamieson, Maj. Gen. Mary O'Brien was named the ensuing deputy chief of staff for Intelligence, Surveillance, Reconnaissance (ISR) and Cyber Effects Operations, which covers Air Force ISR, offensive cyber, defensive cyber, and tactical communications (cyber effects operations capabilities). O'Brien will inherit Jamieson's development of the Air Force's new ISR strategy concerning a sensing grid that fuses data from legacy

platforms (as in RQ-4 and Global Hawk), emerging technologies (as in swarming drones), other platforms. The system is estimated to be functional by 2028. On the other hand, it is still unknown who will lead the "new information warfare numbered Air Force," estimated to be established this coming summer and overseen by Air Combat Command. The new entity will "combine 24th Air Force, Air Forces Cyber, and 25th Air Force combining the service's cyber, electronic warfare, information operations and ISR capabilities under a single entity."
http://tiny.cc/f9gg7y

The Department of Defense's new home for cybersecurity standards

The Defense Information Systems Agency (DISA) launched cyber.mil, a new website providing cybersecurity standards aiding government and commercial organizations to protect the Department of Defense's (DoD) information systems and software. The portal, which also hosts the DoD Cyber Exchange, replaces the Information Assurance Support Environment (IASE) gateway and is only available to those with DoD-issued common access cards. The 350 plus standards are known as Security Requirements Guides (SRGs) and Security Technology Implementation Guides (STIGs) and were designed from Control Correlation Identifiers. Requirements concern vulnerability mitigation, "Information Assurance (IA) controls, security regulations, best practices and [security content automation protocols]," to name the least.
http://tiny.cc/dktg7y
http://tiny.cc/mf0g7y

EUROPE

NATO to integrate offensive cyber capabilities of individual members

During the Cyber Defense Pledge Conference in London, NATO Secretary General Soltenberg revealed some of its strategic direction: "operationalize

cyber capabilities . . . by integrating those tools of member nations." Although representing a continued profile of "defensive in nature, with a mission of deterrence," the organization does not generally engage offensively. However, during the event, Soltenberg stated NATO must be "prepared to use cyber capabilities to fight enemies." Soltenberg additionally noted the significant role attribution plays in the deterrence mechanism, in reference to the "Organization for the Prohibition of Chemical Weapons hack attempt by Russian intelligence operatives."

http://tiny.cc/mxui7y

EU backs cyber sanctions regime, following Dutch and UK pressure

The European Union has added new rules to the Cyber Diplomacy Toolbox (CDT) , which is a framework for a joint EU diplomatic response to malicious cyber activities, adopted in 2017. "The agreement allows the EU to impose sanctions on persons or entities [from non-EU state] that are responsible for cyberattacks or attempted cyberattacks, who provide financial, technical, or material support for such attacks or who are involved in other ways." Such sanctions include "travel bans and asset freezes," in which only "persons or entities" are subjected to, not national governments. The decision is largely a response of an investigation conducted by British and Dutch governments, which uncovered "a range of cyberattacks last year, reportedly originating from the GRU, the Russia military intelligence service." Some of which were associated with the attack on the Organization for the Prohibition of Chemical Weapons (OPCW) in the Hague. Both England and the Netherlands are boldly focusing on implementing and enforcing the measures. Additionally, the UK intelligence services provided "evidence regarding a coordinated hacking campaign conducted by Chinese state-linked group, Advanced Persistent Threat 10 (APT 10)." Although it is unknown to what extent such findings have impacted the catalyst of the recent measures adopted, which seemingly are a response to Russian hacking efforts.

https://bit.ly/2KbJI5W

RUSSIA

NATO warns Russia with possible kinetic response to cyberattacks

After the European Parliament elections kicked off in Britain and the Netherlands, NATO Chief Jens Stoltenberg warned Russia that any meddling in the European elections will draw an immediate NATO response, and the response will not be limited to cyber means and methods. The head of NATO told Russia and other potential foes that the Western military alliance was ready to use all means at its disposal to respond to cyberattacks. "For deterrence to have full effect, potential attackers must know we are not limited to respond in cyberspace when we are attacked in cyberspace," Stoltenberg said during a joint press appearance in London.
http://bit.ly/2HFdmyF

Russia is becoming the biggest market for personal data cyber-espionage

According to cybersecurity experts, vast quantities of supposedly private data—including from Russian state institutions—are bought and sold daily. The market for purchasing personal data in Russia is growing. For a modest fee, one can gain access to mobile phone records, addresses, passport details, and even bank security codes. This is an embarrassing revelation for a country run by former intelligence officer, President Putin, and which prides itself on the excellence and secrecy of its intelligence services. Russia's security apparatus, however, is up against powerful market forces. Officials can supplement their often-meager wages by selling data on the black market, and, according to BBC sources, it is not only Russian citizens whose data can be bought.
https://bbc.in/2QrLZLv

Stolen cyber tool is broadly used by Russia all over the world, including in the United States

Since 2017, when the National Security Agency (NSA) lost control of the tool, EternalBlue, it has been picked up by state hackers in Russia to cut a path of destruction around the world, leaving billions of dollars in damage. Over the past year, the cyberweapon has boomeranged back and is now showing up in the NSA's own backyard. Russia, which used the weapon in an attack called NotPetya, first aimed at Ukraine but then spread across major companies doing business in the country. The assault cost FedEx more than $400 million and Merck, the pharmaceutical giant, $670 million. The damage did not stop there. In the past year, the same Russian hackers who targeted the 2016 American presidential election used EternalBlue to compromise hotel wi-fi networks around the globe.

https://nyti.ms/2YOiXZp

British intelligence: Russia is seeking to undermine state's critical infrastructures, wherever it can

Speaking at the NATO Cyber Defense Pledge Conference in London, Jeremy Hunt, the secretary of state for foreign and commonwealth affairs since 2018 announced that, according to British cyber intelligence, Russia has been engaged in a systematic and malicious global campaign of cyber warfare, targeting critical national infrastructure. "We judge that Russia's intelligence services are targeting the critical national infrastructure of many countries in order to look for vulnerabilities. The UK's National Cyber Security Center has been working with sixteen other NATO states over the past eighteen months to chart how Russia has been looking for vulnerabilities in cyber systems and seeking to compromise government networks," Hunt said. He continued, saying, "This Russian global campaign also seeks to compromise central government networks. I can disclose that in the last eighteen months, the National Cyber Security Center has shared information and assessments with

sixteen NATO allies—and even more nations outside the alliance—of Russian cyber activity in their countries."
https://ind.pn/2W9HTOe

First victim of Russian law of disrespect for the authorities charged

A blogger from Smolensk, Sergei Kommandirov, was apparently arrested and faces charges of an administrative offense for insulting a government representative (part 3 of Article 20.1 of the Administrative Code of the Russian Federation) for publishing a photo of Russia's President Vladimir Putin on the social network with the signature "Every citizen knows who is . . . No. 1." According to the blogger, his post was published in the well-known Russian social network VKontakte. Thus, it is the first application of the "law of disrespect for the authorities" recently adapted by the Russian State Duma and brought into force by Russian authorities. It could be concluded that Russian security authorities, along with the release of such a law, have an overextended cyber infrastructure, including personnel, for tightly tracking internet and social media on Russian territory.
http://bit.ly/30MsQbE

MIDDLE EAST

How Saudi Arabia plans to improve healthcare access in rural areas

Global healthcare technology firm Royal Philips is partnering with the Saudi Telecom Company to arrange a healthcare solution powered by artificial intelligence. The premise of this project is to be able to help patients in remote areas of Saudi Arabia. Philips states that this will allow hospitals and clinics anywhere in the country to be connected to command centers. This will allow doctors in other areas to treat patients remotely. With healthcare in Saudi Arabia free to all citizens, residents, and expatriate workers in the public sector, national healthcare financing is under strain from factors, including

demographic changes, rising costs, and increasing user expectations. Philips said this new cooperation will lead to a much-needed cost efficiency optimization.
http://bit.ly/2HEETQP

Chinese manufacturing giant eyes Abu Dhabi for $10 billion industrial project

East Hope group, a Chinese manufacturing giant, has announced it is working with Abu Dhabi's industrial hub in order to find out about the feasibility of setting up a $10 billion project in the Gulf state. The plan would entail a fifteen-year plan and the lease of 7.6 square kilometers of land on which a three-phased plan could unfold. In the first phase, East Hope would develop an alumina facility. The second phase would include a red mud research center and recycling project. The final phase would see large-scale upstream and downstream non-ferrous metal processing facilities.
http://bit.ly/2wkqFyf

Bahrain to increase penalties for misuse of social media

Mohammed Ibrahim al-Sisi, chair of the Council of Representatives' Committee for Foreign Affairs, Defense, and National Security, said the parliamentary committees' chairs are in the process of studying a bill that includes increasing the penalty for the misuse of social media. This bill, al-Sisi stated, would be in line with Bahrain's government directives to deal firmly with "misuse of social media," which he stated refers mainly to crimes of defamation, insult, spreading rumors, and infringing on individuals, bodies, entities, and state institutions.
http://bit.ly/2VVvbxf

APAC

Huawei launches 5G lab in South Korea but keeps event low-key after US ban

Despite the US backlash against Huawei technologies—banning certain sectors from pursuing business with the tech giant, using their technologies, and trying to influence the international arena to do the same—Huawei nevertheless has opened its Seoul next-generation 5G wireless network lab. "The lab in South Korea is Huawei's first open 5G services development center in the world that will allow other companies to test their platforms, according to the company." Though the event was "low-key" and did not have media present, it was stated the company is planning to invest $5 million in the lab. Huawei's Korea office said "Huawei will build a 5G ecosystem through cooperation with a number of South Korean ICT companies and especially small-and-medium enterprises." The decision illustrates a commitment in South Korea, in particular to the company's component purchasing of chips and screens, and seemingly a response to the broader US-China trade war and its impact on South Korea.
http://tiny.cc/ofzi7y

New Zealand police called in after mass hacking attempt on "wellbeing" budget

Described across the media as "the biggest cyber security scandal to hit parliament," an investigation has been called after the Treasury office reported their systems "had been deliberately and systematically hacked." The attack comes underway as the government was to release its "world first" budget, coined the "wellbeing budget," garnering much domestic and international attention, in which the country's spending priorities will focus beyond economic growth and on mental health, domestic abuse, and child poverty. Over a two-day period, an estimated 2,000 attack attempts were recorded. The news broke a day after the National Party prematurely released some budget-related information. Now claiming the current Labor coalition is steering a "witch-hunt to cover up its embarrassment," the opposition party maintains that it legitimately received the information. Treasury secretary Gabriel Makhlouf disclosed no personal information was at stake and that the "annual budget release would go ahead as planned."

http://tiny.cc/gbqi7y

Foreign Companies in China face cybersecurity crackdown

With efforts to strengthen "national information security," focusing on cloud computing and the Internet of Things (IoT), China has begun investigations on foreign companies operating in the country, particularly in Beijing. Two international firms dealing with consumer data are under official investigation, although more are believed to have been inspected unofficially. In addition, Beijing is set to employ a series of new "cyber rules" under the existing "multilevel protection scheme" (MLPS) implementation requirements of the 2017 Cybersecurity Law. The MLPS regime, which simultaneously reinforces the Cybersecurity Law, is set to expand supervision over technologies, including mobile internet, IoT, cloud computing, big data, and industrial security systems, according to official documents. Kent Kedl of Control Risks, a global risk management firm, notes that he believes the profile targeted in the investigations are the type of associated data, "in this case data around individuals," and added that Chinese firms are also being investigated.
https://on.ft.com/2JIBH87