Global Cyber Bi-Weekly Report by INSS May 01 2019

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

Contributors: Simon Tsipis, Anna Danilova, Gal Sapir, Robin Veldwijk

ISRAEL

Facebook ramps up its Israeli AI operations with new R&D center

Facebook is expanding its artificial intelligence operations in Israel with a new research and development center called Data.AI. located in Tel Aviv's Azrieli Sarona Tower. The new AI team focuses on creating tools for building and improving programs and systems for data processing, which that will assist the work of engineers and programmers. The goal is to enable engineers to access relevant data more quickly and let them work more efficiently. While the products are still in their initial development stages, the idea is that eventually these products would also be made available to other companies.
https://bit.ly/2Vw4JOR

Healthcare has a massive cybersecurity problem, and we're not doing enough to fix it.

Healthcare institutions are glaringly vulnerable to large-scale hacking attacks and we're not doing enough to fix the situation. Healthcare data have enormous value since they contain lots of personal details, including social security numbers and credit card information. Besides monetary and logistical problems, such attacks could also manipulate treatments a patient is supposed to receive, resulting in terrible complications. Hospitals are especially vulnerable because their tech systems are becoming increasingly complicated and interconnected. Although efforts are being made to improve security, better cybersecurity education is needed, more strategic tech replacement standards, and more funding for IT maintenance.
https://bit.ly/2IQRHWf

Israeli IoT cybersecurity co VDOO raises $32m

The Tel Aviv-based IoT cybersecurity company VDOO Connected Trust Ltd., which pioneers security automation for embedded devices of any type, has raised $32 million in Series B financing round, bringing the company's total funding to $45 million. Through this funding, VDOO will be able to increase market adoption of its IoT security platform while also expanding its technical capabilities. The company was founded by co-CEO Netanel Davidi, co-CEO Uri Alter, and VP security Asaf Karas.

https://bit.ly/2UK7uaV

UNITED STATES

White House launches new shared services initiative

One of the major initiations on US president's management agenda is increasing "cross-agency impact," by focusing on "IT modernization, a modern workforce, and data transparency and accountability." Efforts by the Office of Management and Budget (OMB) and the General Services Administration (GSA) have recently transpired in the Centralized Mission Support Capabilities for the Federal Government memorandum, with a core resolve to increase federal agencies shared utility of IT systems and services, estimated to result in over a billion dollars in government cost-savings. Further echoed by the Federal Chief Information Officer Suzette Kent to "help agencies achieve core mission by consolidating redundant administrative functions, eliminating duplicative costs, replacing antiquated technology . . . We're designating lead agencies for a set of common services where we have already agreed on the standards." The emerging policy consists of multiple directives as in the condition for agencies "to appoint a Senior Accountable Point of Contact within the next 30 days to help coordinate actions across agencies." Thus far, the "Treasury for financial management, Health and Human Services for grants management, the General Services Administration for human resource transaction services, and the Department of Homeland Security for cybersecurity services" have been determined as "Quality Service Management

Offices (QSMOs)" and will be conducting planning and implementation stages in the adoption of relevant shared services.

http://tiny.cc/9w9x5y

http://tiny.cc/5y9x5y

Fintech giant Fiserv sued by Pennsylvania credit union for "baffling security lapses"

Fiserv and its competitors Fidelity National Information Services and Jack Henry & Associates are among the top providers of financial services technologies, servicing 90 percent of US banks ("with less than $1 billion in assets"). The company's solutions make up the core of Bessemer System Federal Credit Unions' operations by hosting its website, generating statements, tracking deposits, and processing transactions. The Pennsylvania establishment is seeking compensation for damages caused by the vendor, "including alleged negligence, unfair trade practices, and breach of contract"; notably claiming the Fortune 500 Company's "widespread systematic misconduct," and browbeating if Bessemer discussed the security problems with other parties. In 2018 the fintech giant earned $5.8 billion in revenue, a telling element in one of the multiple complaints made by Bessemer in the lawsuit, which claimed the provider lacked in "proper financial investments to keep up with emerging technology and security risks," not excluding patching vulnerabilities. The supplier has been in the spotlight several times since 2016 in connection to breaches caused by inadequate digital infrastructure security, resulting in the exploitation of hundreds of bank websites and exposure of confidential consumer data in 2018. The lawsuit also references the Wall Street Journal article, "Frustrated by the Tech Industry, Small Banks Start to Rebel," which states, such misconduct "is part of a pattern of victimizing small financial institutions and the consumers they serve."

http://tiny.cc/xs9x5y

A $603 million deal sheds light on cybersecurity space

In the last couple of years, Texas-based Jacobs Engineering Group has acquired cybersecurity firms Virginia-based Blue Canopy and Maryland-based Van Dyke Technology Group, in a continued buying pattern. Recently, the company acquired KeyW Holding Corp. for an estimated $603 million. KeyW was founded by a former National Security Agency senior leader, who later became an executive at Essex Corp., a government defense and intelligence contracting firm. The company provides strategies for "offensive cyberspace operations and training for cyber missions." Both Jacobs and KeyW have established histories with "cyber intelligence specialists" from Washington DC and are closely associated professionally with the government in facilitating intelligence collection via aircraft and satellites. A little over 20 percent of Jacobs' $15 billion revenue is earned from the US government. The acquisition prescribes enhanced government access.

http://tiny.cc/629x5y

EUROPE

Huawei: US official warns "no safe level" of involvement with tech giant

Huawei technologies are largely banned from use by the US government and by government contractors, and face business contract restrictions in many foreign countries due to concerns of the company's ties to its government. Recently, information was leaked from United Kingdom's National Security Council, revealing the "government had decided to allow the Chinese telecoms firm to have a limited role in bringing 5G to the UK [the non-core parts of its 5G network]". The United States is aggressively leading the efforts among foreign governments in limiting the firm's mobility in the transition to the fifth generation of mobile internet connectivity. Rob Strayer, deputy assistant secretary for cyber and international communications at the US State Department, said "this is truly a monumental decision being made now . . . we think there's unacceptable risk in letting untrusted vendors provide that base

infrastructure because they could disrupt any of those critical services." Various reports illustrate Prime Minister Theresa May's senior cabinet ministers cautioning the provocative decision. Mr Strayer said the US was informing other countries that if they put unsecure and untrusted vendors into their 5G networks, "in any place" then it was "going to have to consider the risk that produces to our information-sharing arrangements with them." The official spokesman for the prime minister conveyed that "where national security concerns arise in any foreign investment the government will assess the risks and consider what course of action to take."
http://tiny.cc/5ooy5y

UK cybersecurity agency won't tip regulator on breaches

The UK cybersecurity agency, National Cyber Security Centre (NCSC), will not instinctively share information about data breaches with the country's data privacy regulator, the Information Commissioner's Office (ICO). The decision is a response to the European Union's General Data Protection Regulation, which enables national regulators, as in the ICO to enforce fines up to 4 percent of global revenue for data breaches. Further "to prevent . . . [contrasting] effects on businesses' willingness to share information about cyber-attacks with the government." According to the NCSC "the new policy puts the NCSC in the potentially awkward position of knowing about violations of data privacy laws and withholding that information from other parts of government. The NCSC said that while it would not notify the ICO of breaches without permission, it would encourage organizations coming to the agency to comply with the law."
http://tiny.cc/lsoy5y

RUSSIA

Facebook and Twitter fined in Russia for not providing the exact location of their servers

Personal data of Russian users must be localized in Russia in accordance with the Russian new law, which went into effect from September 2015. Companies are obliged to keep personal information of Russian users and citizens only on servers located within the country. According to Russian authorities, Facebook and Twitter failed to provide information on the location of Russian user's data within thirty days after the law was issued, and thus, both social networks were fined by 3,000 rubles each.

http://bit.ly/2UKmPYX

http://bit.ly/2GCVi6K

Russia to hold annual national cybersecurity forum in Kazan

From May 29 to 31, more than a thousand experts in the field of digital technologies will gather in Kazan at the thirteenth all-Russian IT & Security Forum (ITSF). This is an annual digital forum held by ICL System Technologies. It is intended for professionals and managers responsible for digital transformation and meeting the requirements of Russian legislation in the field of ensuring the cybersecurity of their enterprises and organizations. The key partners of the forum in 2018 were Kaspersky Lab, Dell EMC, Check Point Software Technologies, and Zecurion.

http://bit.ly/2Lac82o

State-owned companies will be banned from using foreign databases and hardware

In the draft law of the Russian "Sovereign Internet," called Runet, experts discovered a rule that would complicate the life of state-owned companies: They are forbidden to use foreign databases and PC and IT equipment. The ban could have a negative impact on Russia's leading long-distance telephony provider, Rostelecom. State structures (corporations, federal state unitary enterprises, and so forth), as well as state bodies that are operators of any information system, will not be able to use foreign databases and equipment stationed or manufactured abroad. Such a provision is contained in a bill approved by the Russian parliament, which received the unofficial name

"Federal Law on the Sovereign Runet." The document was approved by the Russian State Duma and the Federation Council but has not yet been signed by the Russian president and has not been officially published.
http://bit.ly/2vs3pxC

The Russian state-owned "Sovereign Internet" project is on the way

The share of Russian-made software in the procurement of government agencies has reached 65 percent, in comparison to 2015, when the share was 20 percent. According to the calculations of the Ministry of Communications and Mass Media, by 2024 the share of Russian software will increase to 90 percent in the procurement of state bodies, and up to 70 percent in the procurement of state companies.

The Ministry of Communications and Mass Media issued measures to stimulate the transition to state-owned companies' domestic software, including the directive from December 6, 2018, signed by the first deputy chairman of the Russian government, Anton Siluanov. According to the directive, state-owned companies should plan a phased transition to domestic software. Import substitution of foreign software is also being implemented in the field of public procurement of telecommunications equipment. At the moment, a draft government decree that will limit government procurement of foreign radio-electronic products is already under interdepartmental coordination. Also, the Russian authorities intend to issue directives that prescribe primarily Russian software equipment while funding the creation of additional infrastructure at state expenses.
http://bit.ly/2J08Ls4

APAC

Japan, United States beef up their cyber alliance

Washington and Tokyo have vowed to intensify their cooperation on cybersecurity, while signaling that the United States could come to the aid of Japan if it faced a serious computer-based attack. In a joint statement issued after a "two-plus-two" meeting in Washington, DC, between Mike Pompeo, the US secretary of state, and Patrick Shanahan, the acting US defense secretary, together with their Japanese counterparts, Foreign Minister Taro Kono and Defense Minister Takeshi Iwaya, the Ministers expressed concern about "rapidly evolving technological advancement in new domains, including space, cyberspace, and the electromagnetic spectrum." The focus on cybersecurity reflects growing concerns among policymakers about the potentially devastating impact of attacks on critical infrastructure or communication networks, at a time when businesses, utilities, government entities, and the general public are increasingly reliant on digital technology. Japan's latest annual defense white paper said state-sponsored cyberattacks had been on the rise in recent years and were becoming more sophisticated. During the April 19 meeting, the ministers "affirmed that international law applies in cyberspace and that a cyberattack could, in certain circumstances, constitute an armed attack for the purposes of Article V of the U.S.-Japan Security Treaty." A decision as to whether a particular cyberattack rose to that level of seriousness would be made on a case-by-case basis.
https://bit.ly/2J1mxKR

Highlights of China versus Amnesty International Hong Kong cyberattack

Hong Kong is a Special Administrative Region, with its own internal ministerial government directly elected by the Hong Kong people. Now hacker groups allegedly linked with Beijing are hitting Hong Kong-based Amnesty International. "Cyber forensic experts were able to establish links between the infrastructure used in this attack and previously reported APT campaigns associated with the Chinese government," stated Amnesty International. Security experts believe that the organization was hit with an APT campaign, usually pulled off by professional hackers who are employed by a state.

https://bit.ly/2ZKZXfo