Global Cyber Bi-Weekly Report by INSS June 15 2018

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

Contributors: Simon Tsipis, Ido Sivan, Anna Danilova, Sneha Mukherjee, Bryan McCarthy, David libin

ISRAEL

The IDF hosted its first international digital and cyber convention

The C4i and Cyber Defense Directorate of the Israel Defense Forces held its first international digital and cyber conference. Chief Signal Officer and J6/C4I and Cyber Defense Directorate Chief of Staff Brig. Gen. Yariv said at the event: "This conference brought dozens of representatives to Israel to discuss operational and technological challenges that all modern armies experiences or will experience in the future. We need to work together in order to protect ourselves better and to operate in synchronization." About seventy foreign representatives from eleven countries (South Korea, the United States, Austria, Britain, Canada, the Netherlands, Italy, Rwanda, Japan, Hungary, and Poland) attended the conference, including six generals and sixteen colonels who deal with cyber and military defense technology. During the conference, which was held at the C4i Corps' heritage site in Yehud, participants learned about Information and Communication Technology (ICT) development, technological challenges on the battlefield, and appropriate responses to them. In addition, they learned about digital transformation (DT), both in cyber technology and in the cloud.

https://bit.ly/2JLWIPW

Israeli cybersecurity companies are on the rise

Israeli cybersecurity firms have raised an approximate $814.5 million in eighty-one deals in 2017 in both venture capital funds and private equity deals, according to a new report on Israel's cyber sector by Start-Up Nation Central. This is a record-

breaking amount for the third year in a row and has even exceeded 2016 investments by 28 percent. Israel's cybersecurity industry comes second only to the United States, accounts for around 16 percent of the total cybersecurity investments made worldwide, and has slightly increased its share from around 15 percent in 2016. In addition, fourteen Israeli cyber companies made exits in 2017, including buy-outs, IPOs, and acquisitions. An example of cybersecurity deals protecting the online identity and information of individuals and organizations is Skybox Security. According to Nir Falevich, head of the cybersecurity sector at Start-Up Nation Central, the increased adoption of the Internet of Things (IoT)—with more and more devices connecting to one another—"poses new and significant threats for enterprises, nations, and individuals." Falevich said that "during 2017, Israeli entrepreneurs and investors put many resources in offering solutions to protect IoT networks and devices."

https://bit.ly/2HJR0Jj

USA

The Cybersecurity 202: "If you don't have a brand, you're not in the game." New DHS cyber chief wants to rename his agency

The Washington Post has reported that the Department of Homeland Security's (DHS) National Protection and Programs Directorate will soon be changing its name to something closely resembling its actual task is. As new director Chris Krebs says, "I need a name on the door that tells what the organization does." One of the names suggested is Cybersecurity and Infrastructure Security Agency. Even though there is broad bipartisan support for a name change and possible elevation of the department, the process of changing the name and status has been delayed due to typical turf wars among Senate committees and legislative priority.

https://wapo.st/2LRfB1n

The Cybersecurity 202: Voter confidence is the biggest election security challenge, DHS cybersecurity official says

A top DHS cybersecurity official has warned that the biggest security issue going into the midterm elections is not technical but rather psychological. As Matt Masterson says, "To me the number one threat is around public confidence in the process." Masterson is pushing for DHS to provide funds and information to state election bodies in order to confront both technical security issues and information issues. The top priority of these is informing the public that when they go to the polls, their votes are secure.

https://wapo.st/2JEkeiH

North Korea's nuclear threat is nothing compared to its cyber warfare capabilities

Morgan Wright posits in the Hill that the top priority at the Singapore Summit held on June 12 between President Trump and Kim Jong Un should have been the cessation of offensive North Korean cyber operations and not denuclearization. As he said, "a nuclear attack against the United States by North Korea would be 'one and done', while a cyberattack by North Korea is the gift that keeps on giving for Kim Jong Un. The former was never really a reality in our lifetime." The author continues to list North Korea's many visible cyberattacks and cryptocurrency thefts and the need of the Trump administration to immediately and firmly counter these attacks.

https://bit.ly/2M2zIKS

EUROPE

EU parliament overwhelmingly backs recommending a ban on Kaspersky products

A huge majority of EU lawmakers backed a cyber defense resolution to boost cooperation between the EU states and NATO, citing threats from Russia, North Korea, and China. The resolution was passed with 476 members of the European

Parliament voting in favor, 151 voting against, and 36 abstaining. Although not binding, the resolution could spell more trouble for Kaspersky Lab as it calls on Europe to ban its antivirus in EU institutions. This follows a US ban on Kaspersky Lab's antivirus in the government after US officials accused the company of working with Russian intelligence. Kaspersky Lab has denied those allegations.

https://bit.ly/2sWeCWC

Nation-state cyberattacks threaten everyone, warns ex-GCHQ boss

The dynamics of cyber warfare have changed so dramatically that nation-state attacks are now a problem that everyone needs to face, the former head of the UK intelligence agency, the General Communications Headquarters (GCHQ) has warned. "Five years ago we were aware of nation-state attacks but we would've seen them as something that only a nation-state needs to worry about. Today they're a problem for everybody, as we've seen over the last year," said Robert Hannigan, who served as director general of GCHQ from 2014 to 2017.

https://zd.net/2xVyptV

Britain's Dixons Carphone admitted a huge data breach

Dixons Carphone has admitted a huge data breach involving 5.9 million payment cards and 1.2 million personal data records. British mobile phone and electricals retailer admitted that on June 13, it became the latest victim of cybercrime after discovering unauthorized access to its payment card data. "We have taken action to close off this access and have no evidence it is continuing. We have no evidence to date of any fraudulent use of the data as result of these incidents," according to the company. Its ongoing investigation indicated there was an attempt to compromise 5.9 million cards in one of the processing systems of Currys PC World and Dixons Travel stores.

https://cnb.cx/2t9A7lS

Spanish football league defends phone "spying"

Spanish football league La Liga has defended the privacy policy of its app after admitting it was accessing the microphone and GPS of Android users. It said it had been trying to track down venues that illegally broadcasted matches, by matching audio data and phone location. The app, downloaded more than ten million times on the Google Play Store, has been criticized by fans. La Liga said it wanted to "protect clubs and their fans from fraud."

https://bbc.in/2JCGDg7

RUSSIA

Putin: Blocking Telegram was due to anti-terrorist measures

During his annual "direct line" broadcast, Putin said that the Telegram messenger app was blocked for national security reasons. The Federal Security Service could not track the terrorists' correspondence following the Saint Petersburg's terror attacks in metro in April 2017, as a result of being encrypted by Telegram, which refused to decrypt them.

http://bit.ly/2MqEMc2

Did Russian hackers attack German energy infrastructure?

The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik [BSI]) announced a series of cyberattacks against the country's energy enterprises. As the BSI believes, the attacks could be associated with Russian hackers. According to the agency, this is a large-scale attack, aimed at energy companies. Hackers have already managed to penetrate the networks of several enterprises. BSI does not disclose information on the exact number of companies affected; however, according to some reports, traces of attacks have been found in networks of more than a hundred firms.

http://bit.ly/2l9qUXb

Russian Ministry of Defense to launch its own "military internet" by 2020.

The Russian Ministry of Defense intends by 2020 to launch its own secured cloud service that will host all the ministry's information. The project of launching the Russian "military intranet" has cost already an estimated 390 million rubles (around $6.3 million). The system will be divided by military districts. The facilities will be highly secured, with strictly limited access, specially trained personnel, and special cybersecurity features, such as blocked access of unauthorized USB plug-ins and strictly Russian-produced software. The intra-mail service will be limited only to the internal internet (intranet) network.

http://bit.ly/2JQCR27

Russian Ministry of Defense radically is toughing cybersecurity measures

According to new decree of the Ministry of Defense of the Russian Federation, entry into the territory of departmental regime organizations with electronic devices is now prohibited. It is now forbidden on the territory of departmental facilities, as well as the organizations dealing with state secrets, to carry smartphones, telephones with cameras, photo and video equipment, smart watches, fitness trackers, and even push-button mobile phones. The ban also includes any devices with Wi-Fi, Bluetooth, infrared ports, mobile modems, and devices with the ability to determine location.

http://bit.ly/2JVV12c

CHINA and APAC

Latest theft of navy data another sign of China targeting defense companies

Earlier this year, Chinese hackers broke into the computer systems of a US navy contractor, stealing a trove of data on American weapons systems. The 614 gigabytes of data taken from an unclassified network could undermine the fighting ability of US submarines. The intrusion and theft, first reported by the Washington

Post, were yet another hack in the more than decade-long campaign by Chinese intelligence in targeting US defense companies to close the technology gap as China tries to become a US military peer. China had paired its hacking of military technology with stealing commercial technology to help Chinese companies, but in 2015 China promised to cut down on its theft of American intellectual property; however, it did not include spying on military hardware.

https://bit.ly/2HT08vi

Vietnam cybersecurity law to restrict Facebook and Google

Vietnam has approved a restrictive cybersecurity law that will force Google, Facebook, and other tech companies to store their data in-country, which the industry said would hurt investor confidence and stunt the growth of the country's digital economy. Activists, who staged demonstrations protesting against the law and other issues, said the new requirements would allow communist authorities to access private data, spy on users, and erode the limited freedoms of speech enjoyed by citizens. Foreign tech companies, many of which operate regional hubs in Singapore or Hong Kong, would need to open a Vietnam office and store their data there. They will also be required to provide users' data to the public security ministry at the government's request in cases where it believes the law is being violated. These provisions will result in severe limitations on Vietnam's digital economy, dampening the foreign investment climate, and hurting opportunities for local businesses and small and medium sized enterprises to flourish inside and beyond Vietnam," said Jeff Paine, the group's managing director. The new law takes effect from the start of next year.

https://on.ft.com/2ygzKMe

Security experts warn hackers will target Americans traveling to Russia for World Cup

Top security officials are warning Americans who traveled to Russia for the 2018 FIFA World Cup that Moscow-linked hackers may try to target them as they attend the

international soccer event. The officials say US travelers should be extra cautious about what devices they bring, which servers they connect to, and the types of data they access while in Moscow. When it comes to Russia, Russia— more than any country in the world—is one of the most well-versed in cybercrime, both from the organized crime side and their intelligence networks in the world," said Robert Anderson, a former national security executive at the FBI who now serves as a security expert with the Chertoff Group.

https://bit.ly/2t24NXc

Ottawa unveils new cybersecurity strategy targeting public and businesses

The federal government is rolling out a new cybersecurity strategy. The plan was supported by $500 million over five years, which was included in this year's federal budget. Those include the establishment of a new Canadian center for cybersecurity, a certification program for small businesses that want to shore up their cyber defenses, and more resources for the Royal Canadian Mounted Police to tackle online crime. The plan, which is an update to Canada's first cybersecurity strategy in 2010, faces at least one immediate hurdle: a shortage of cybersecurity specialists that makes it difficult for the federal government and others to recruit talent. The government hopes that positioning Canada as a world leader on cybersecurity not only will address that problem but will also add an estimated 11,000 jobs and $1.6 billion that the sector already reportedly generates each year. The plan is also largely silent about foreign-owned telecommunications companies, such as Huawei, which intelligence chiefs in the United States have identified as a national security risk.

https://bit.ly/2tbwhIT

USB-powered fans for journalists in Singapore: A cybersecurity threat?

Journalists at the US-North Korea summit in Singapore were given USB-powered fans, causing some alarm from those wary of malware that can be easily transmitted by USB devices. While it appears that the fans did not include any storage or

processing capabilities able to transmit malware, they present an interesting example of how creative hacker or a sponsoring government might target victims. "There's an adage in cyber security: if you give someone physical access to your computer, it's no longer your computer. Use an unknown USB stick and you are doing just that."

https://bit.ly/2MtF8P8

AFRICA

Financial losses for African countries due to ransom

Financial losses for African countries continue to remain high, with Nigeria losing 649 million annually and Kenya losing 210 million annually. Companies are often paying the ransom costs in order to retrieve their data. The large amounts of pirated software in Africa make enforcing intellectual property laws difficult. Financial institutions, E-commerce, and government are the organizations most attacked. The loss of customer confidence due to cybercrime is a large impediment to the expansion of African business.

https://brook.gs/2Jm08bV

Nigerian ministries, departments, and agencies choose not to work with Office of the National Security Advisor on cyber infrastructure

Ministries, departments, and agencies (MDAs) of Nigeria, are not working with the Office of the National Security Advisor (ONSA) on matters related to cybersecurity as they fear that they will be exposed to spying. However, ONSA has capabilities that these MDAs should consider helpful for their operations. The lack of training and coordination has left Nigeria unprepared for the increasing developments in IoT technologies entering the country. The need for more local cybersecurity certifications, to compliment international ones is necessary to further readiness says Daniel Adaramola, an official at the information technology unit of Heritage Bank.

https://bit.ly/2y08jX4