Global Cyber Bi-Weekly Report by INSS March 1 2018

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

Contributors: Simon Tsipis, Ido Sivan, Sanjana Rathi, Anna Danilova

ISRAEL

IDF's Unit 8200 helped Australia thwart attempt to bomb plane

The IDF cleared for publication that the Military Intelligence Directorate's Unit 8200 helped Australia thwart an attempt to bomb a commercial plane last year. "Unit 8200 provided exclusive intelligence that led to the thwarting of an airliner bombing by Islamic State (ISIS) at the end of 2017." In an interview with *Ynet* around the time of the thwarted attack, IDF Chief of Staff Gadi Eizenkot said, "Since our intelligence capabilities are the best in the area, and certainly in Israel's close vicinity, we contribute to the effort to defeat ISIS and the Nusra Front. We do with this our allies, sharing intelligence to support this effort. We pass on information to countries when we know something is in the works (in those countries). The (Israeli) intelligence community greatly contributes to thwarting terror attacks in the Middle East and elsewhere around the globe." A senior Unit 8200 explained that "a part of 8200 deals with operational activity beyond the borders. Our missions include incorporating offensive cyber tools as well as tools that help shape perception, alongside cyber defense. The cyber world has become a tool to achieve military and diplomatic goals. Today, it's not just about reaching arenas like Syria and Iran, but also to bypass technological giants without getting caught." He said technologies and tools developed in the unit allowed Israeli forces to thwart dozens of terror attacks in the West Bank, mostly those planned by lone wolf terrorists. "We run advanced algorithmic in a technological machine that constantly learns and develops the more data you input," he said.

goo.gl/iKmZh6

Talent, trust and trade in cyber

"Once it was a disadvantage to say you are from Israel. Today when you talk about cyber or advanced technologies, it is an advantage!" said Prime Minister

Netanyahu last year at an international cybersecurity conference. Indeed, few can deny Israel's technical talent, and many Israeli companies have used that reputation to attract investment and customers. But Israel needs to plan for a future where cybersecurity requires political trust as much as quality technology. The importance of political trust was demonstrated by the recent veto of a large commercial transaction by US regulators. To compete in the world market, Israeli companies need to cultivate a meticulous reputation for smart and sophisticated data privacy and data security. Israel needs to update its international trade agreements to allow for cross-border data transfers. Other countries have begun to consider incorporating such provisions in their own trade agreements, and Israel needs to ensure that its interests are not left behind. Israel has a formidable reputation for technological excellence, but that reputation will not itself support commercial success. Our talent must be complemented by a reputation for neutrality, privacy, and security.

goo.gl/Qm6foP

UNITED STATES

US official who focused on election security will be replaced

The head of a federal commission who has helped the United States protect its election systems from possible cyberattacks by Russia or others is being replaced at the behest of Republican House of Representatives Speaker Paul Ryan and the White House.

https://goo.gl/bkhQ5P

United States is preparing "bloody nose" cyberattacks on North Korea

The United States is drawing up plans for cyberattacks on North Korea to bring the regime of Kim Jong-un to heel, according to intelligence sources, as Pyongyang said it is ready for "both dialogue and war" with the culmination of the Winter Olympics. Washington's potential plans for a series of "bloody nose" attacks on targets in North Korea, as revealed by the *Telegraph*, could focus on digital rather than conventional warfare. A cyber assault could cripple Pyongyang's online communications and ability to control its military, causing huge disruption but avoiding the loss of life. It may also assuage

concerns that a conventional attack against missile sites or nuclear facilities by the United States could trigger a massive counter-strike by Kim Jong-un.

http://bit.ly/2HRqrmT

US Securities and Exchange Commission calls for "clearer" cyber risk disclosure from companies

The US Securities and Exchange Commission updated its guidance for public companies on how and when they should disclose cyber security risks and breaches, including potential weaknesses that have not yet been targeted by hackers. The guidance also said company executives must not trade in a firm's securities while possessing nonpublic information on cybersecurity attacks. The SEC encouraged companies to consider adopting specific policies restricting executive trading in shares while a hack is being investigated and before it is disclosed.

http://reut.rs/2BVi0pO

EUROPE

Just 8 percent of UK small businesses are GDPR-ready

The Federation of Small Businesses (FSB) has launched a new General Data Protection Regulation (GDPR) awareness campaign after revealing that just 8 percent of the smallest firms in the United Kingdom are prepared for the new EU privacy regulation. It revealed that over a third of sole traders (37 percent) and micro-businesses (35 percent) have not yet started preparations for the GDPR, while 18 percent of UK small businesses have not heard of the regulation at all. Some 35 percent are still only in the early stages of preparing for the new regulation which represents the biggest change to the region's privacy laws in a generation. Those in arts and entertainment are least prepared, with over half (52 percent) not having started compliance efforts. At the other end of the scale are financial services firms, 82 percent of which have either started or completed their work.

http://bit.ly/2F7nfol

Cybercrime becomes most common form of fraud in United Kingdom

For the first time ever, cybercrime has been reported as the most common form of fraud for businesses in the United Kingdom. While declining five percent from 2016, fraud was still rife in the United Kingdom in 2017 with 50 percent of businesses being victimized. This is according to PwC's 2018 Global Economic Crime Survey, which revealed cybercrime as the most commonly experienced fraud after overtaking asset theft. Even more concerning is the fact that 49 percent of UK fraud was related to cybercrime compared to 31 percent globally.

http://bit.ly/2t093J5

British lawmakers are launching an inquiry into cryptocurrencies

Britain's cross-party Treasury Select Committee of lawmakers on Thursday said it is launching an inquiry into digital currencies, as well as the underlying distributed ledger technology. The probe will focus on the opportunities and risks posed to consumers, businesses and the government by the rising popularity of cryptocurrencies, the committee said in a statement. The inquiry will consider whether the government is striking the right balance between protecting customers and businesses while encouraging innovation.

http://cnb.cx/2on90RY

European regulator proposes hack protection, geo-awareness for drones

The European Aviation Safety Authority (EASA) has proposed anti-hacking measures and geo-awareness technology for small drones to avoid collisions with aircraft or people, taking an important step toward Europe-wide regulations. The reworked proposal published by the EASA)=, which will be the basis for the European Commission to adopt concrete rules later in the year, includes requirements for drones to be remotely identifiable and to recognize when they stray into banned areas. With demand booming—both for hobby and commercial use— European regulators have been looking for ways to ensure drones can be safely operated, while allowing the industry to grow.

http://reut.rs/2t2bFpJ

Criminals hide "billions" in cryptocurrency, Europol warns

Europol, the European Union's law enforcement intelligence agency, estimates that criminals in Europe generate $140 billion in illicit proceeds annually, of which about 3 or 4 percent or $4 billion to $6 billion is being laundered via cryptocurrencies. "It's growing quite quickly and we're quite concerned," Rob Wainwright, Europol's director, told BBC Panorama. Bitcoin is not the only cryptocurrency used by law-abiding virtual currency aficionados as well as those involved in illegal activities. Europol's most recent Internet Organized Crime Threat Assessment warned that "while the abuse of bitcoin remains a key enabler for criminal conduct on the internet, a number of other cryptocurrencies are beginning to emerge in the digital underground," including monero, ethereum and zcash.

http://bit.ly/2FBeot4

RUSSIA

Russian hacker promised to prove FSB links to cyberattacks during US elections

Yekaterinburg hacker Konstantin Kozlovsky, who is accused by the Russian authorities of stealing billions of rubles from bank accounts, which the Moscow City Court kept under arrest until May 18, 2018, made a sensational statement that he was working under the instructions of the Federal Security Service (FSB) of Russia and is ready to publicly prove the involvement of Russian special services in breaking into the servers of the US Democratic Party and the personal electronic correspondence of Democrat candidate Hillary Clinton and Russia's interference in the US presidential elections in 2016.

http://bit.ly/2omsrKR

German defense minister: Russia is the key player in the future global threat assessment

At the Munich Conference, the Defense Minister of the Federal Republic of Germany Ursula von der Läien declared cyberattacks as the main threat to global stability and ambiguously hinted that Russia is the main threat in this field.

http://bit.ly/2ocm7Gv

Russian security official: Russia soon to be under unprecedented cyberattacks

The Secretary of the Security Council of the Russian Federation Nikolai Patrushev stated that foreign intelligence agencies are preparing to hit Russia with major cyberattacks. The Security Council secretary also reported that more than 500,000 computers were disabled during three massive attacks using malicious software. According to him, the information systems of the Ministry of Internal Affairs of Russia, and the Rosneft and Evraz companies were infected by cryptographers. "In 2017, there were three incidents of mass implementation of software that encrypted user's data. As a result, more than half a million computers were disabled, including the information structure of the Russian Federation," Patrushev noted.

http://bit.ly/2sMBev8

MIDDLE EAST

Extensive surveillance by the Iranian regime is revealed

New cyber revelations from the People's Mujahedeen of Iran (MEK), the Iranian opposition movement, about the scope of mass surveillance by the Iranian regime show the desperation of the regime in confronting the nationwide uprising that began last December and has continued to this day. Only when the Iranian regime employed cyber technology was it able to slow down the spread of the protests and wage a large number of arrests. Technology played a significant role in organizing protests, exchanging information between different locales, and getting their message out to the rest of the world. The protests expanded even as the regime desperately cut off access to the internet and blocked key mobile apps, such as Telegram. In response, the regime has focused on mass surveillance through malicious codes embedded in IRGC mobile apps. The goal was to monitor and disrupt the communication between protesters and dissidents. Tehran also apparently

used foreign assistance to advance its cyber warfare. On September 4, 2012, the state-run Fars News Agency reported that the "signing of an agreement between Iran and North Korea to confront cyberattacks has raised concerns in the west."

http://bit.ly/2EM0ozs

Saudi foreign minister admits Iran to be the most serious cyber threat

The most dangerous nation for cyber threats is Iran, according to Saudi Foreign Minister Adel Al-Jubeir. "Iran is the only country that has attacked us repeatedly and tried to attack us repeatedly. In fact, they tried to do it on a virtually weekly basis." Al-Jubeir's statement was not surprising, given the mounting animosity between the Sunni monarchy and the Shiite Islamic republic. The Iranian government did not respond to Al-Jubeir's comments, but it has denied accusations of aggression in the past. Speaking at the sidelines of the Munich Security Conference, the foreign minister repeatedly criticized Iran for what he called "mischievous behavior" in the region, referring to its support for the Shiite militant group Hezbollah, which holds influence in Lebanon and elsewhere in the Middle East. Al-Jubeir said his country was taking steps to combat the perceived cyber threat from Iran. "We are taking all the steps necessary to provide defenses for our data banks and for our internet . . . and also to train our own people in order to be able to engage in offensive operations to make it hopefully impossible for people to penetrate those systems," he said.

http://cnb.cx/2HsPQ66

Iran could be soon spying on smartphones worldwide

Millions of smartphone users in the United States and around the world are vulnerable to being spied-on by the Iranian government, according to a new report. Apparently all it takes is downloading the wrong app. The report was recently published by the National Council of Resistance of Iran (NCRI), considered to be the nation's largest opposition group. NCRI researchers allege that hundreds of smartphone apps currently are being used by the Iranian regime to spy on its own citizens, some of them are available to users around the world via online marketplaces like Apple's App Store, Google Play, and GitHub.com. GitHub's company policy on malware suggests they "do not

allow anyone to use our platform for exploit delivery, such as using GitHub as a means to deliver malicious executables." While the policy prohibits anyone from using the GitHub platform to distribute apps with malicious code, GitHub goes on to state that the company does not "prohibit the posting of source code which could be used to develop malware or exploits, as the publication and distribution of such source code has educational value and provides a net benefit to the security community." The NCRI report lists a handful of supposedly problematic apps available outside of Iran, despite the alleged connections to Iranian intelligence. The list includes Mobogram, Telegram Farsi, and Telegram Black. Fox was able to confirm that most, if not all, are indeed still available for download. Thousands of people were arrested during the protest period, and the NCRI suggests some of them were presented with the option "to leave the Telegram environment and enter the controlled environment of Mobogram" before being released by authorities.

http://fxn.ws/2onLSD3

CHINA and APAC

India's City Union Bank CEO says bank suffered cyberattack via SWIFT system

Cyber criminals hacked the system of India's City Union Bank and transferred nearly $2 million through three unauthorized remittances from accounts in Dubai, Turkey, and China, to lenders overseas via the SWIFT financial platform. The CEO called this a conspiracy involving multiple countries and added that lender was still investigating how it had happened. Furthermore, the Brussels-based SWIFT has been urging banks to bolster security of computers used to transfer money since Bangladesh Bank lost $81 million in a February 2016 cyber heist that targeted central bank computers used to move funds. Also, banking security experts have warned that Indian banks that rely on the SWIFT messaging platform needed to be more vigilant as one hundred financial institutions in India are connected to SWIFT, which includes the Central Bank.

http://reut.rs/2CuEGtL

Australian universities targeted by Iranian hackers

According to Michael Sentonas, vice president for technology strategy of CrowdStrike, geopolitics is driving a lot of the cyberattacks lately. CrowdStrike

has referred to this as "cyber statecraft" in their 2018 Global Threat Report. Sentonas added that Iran has a specific interest in Saudi Arabia as there are a number of diplomatic disputes. Iran, which is heavily embargoed, wants access to intellectual property, which they may not necessarily be able to get. Groups that are linked to Iran seek that information, and therefore target Australian universities with cyberattacks.

http://zd.net/2oBxR4B