Global Cyber Bi-Weekly Report by INSS February 15 2018

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

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

ISRAEL

Polish electric company looks to Israel as "partner in fighting cybercrime"

Israel Electric Corporation will provide technology and assistance to Poland, which is concerned with protecting its electricity infrastructure from cyberattacks. A delegation sponsored by Poland's Polskie Sieci Elektroenergetyczne, headed by CEO Eryk Kłossowski, arrived in Israel last week to sign the cooperation agreement under the auspices of the Cyber Division of the Israel Export Institute. Poland initiated the contact with the Export Institute, seeking help in defending its infrastructure from cyberattacks, the Israeli organization said. The vulnerabilities of critical infrastructure networks were highlighted last week when Israeli cybersecurity firm RadiFlow discovered that a hacker had invaded a European water company's automated supervisory control and data acquisition network—generally used to manage infrastructure networks like electrical grids and water distribution systems—in order to mine cryptocurrency. The Polish electric company, with some 40 million customers, hopes to avoid a similar fate, said Kłossowski. In working with the Israel Electric Corporation, "we gain an experienced partner, effective in fighting cybercrime. This is extremely important at a time when cybercriminals and cyber terrorists develop cooperation among themselves and create more and more advanced tools of attacks," he added.

goo.gl/PCtzty

Israel hosts first international cybersecurity conference for cities

Cybersecurity and technology officers from eighty municipalities worldwide are heading to Tel Aviv to attend the First International Cyber Security Conference for the Municipal Sector, with the aim of learning how to keep

their connected cities safe from the hundreds of daily cyberattacks that can immobilize critical infrastructures. Among the activities will be simulated war-games, sessions on cyber defense strategies, and an introduction to current and future technologies. Experts in the cybersecurity industry will present various innovative tools of defense and cyber-threat assessment.

goo.gl/ZUTLuJ

Cyberwar nightmares: How can Iran, Hezbollah use cyber to fight Israel?

In estimating the cyber dangers potentially posed by Israel's adversaries, the primary focus is on Iran and Hezbollah, which are considered inferior to Israel in the cyber realm but are serious threats on a playing field where agile cyber offense almost always inevitably beats stagnant cyber defense. Israel's adversaries could potentially hack the Israel Air Force aircraft, including the new, most advanced F-35. The *Jerusalem Post* also has reported that a project has started to replace "smart" engines with closed-off, or "dumb," engines, so that if such a hack occurs, only information—not the engines—can be hacked. The flip side of this is that IDF Brig. Gen. (ret.) Yair Cohen said the IDF could potentially disable an entire squadron of enemy aircraft using cyber weapons. Israeli drones can also be hacked and already have been. To date, Iran and Hezbollah have failed to hack Israel to the same extent that Russia and China have managed to hack the United States and Europe. Also, Israel has had the opportunity to study many cyberattacks, which has helped it adapt and build better cyber defenses. Finally, Israel's cyber offense still overshadows that of its adversaries, and a counterattack could block cyberattacks by its adversaries from having more than a temporary impact. But in looking at cyber threats in the next war, Iranian drones and Hezbollah rockets are far from the only surprises Israel may face.

goo.gl/uqVMLY

United States

US Democrats push $1 billion bill for election security

Congressional Democrats introduced legislation that would provide more than $1 billion to boost cyber security of US voting systems, and Vice

President Mike Pence defended the administration's efforts to protect polls from hackers.

http://reut.rs/2F80iPL

US Energy Department forming cyber protection unit for power grids

The US Department of Energy (DOE) said it is establishing an office to protect the nation's power grid and other infrastructure against cyberattacks and natural disasters. President Trump's budget proposal unveiled this week included $96 million in funding for the Office of Cybersecurity, Energy Security, and Emergency Response. Energy Secretary Rick Perry said the DOE "plays a vital role in protecting our nation's energy infrastructure from cyber threats, physical attack and natural disaster, and as secretary, I have no higher priority."

http://reut.rs/2ClN4Md

US senators concerned about Chinese access to intellectual property

China is trying to gain access to sensitive US technologies and intellectual properties through telecommunications companies, academia, and joint business ventures, US senators and spy chiefs warned at a Senate hearing. Republican Senator Richard Burr, chairman of the Senate Intelligence Committee, said he worried about the spread in the United States of what he called "counterintelligence and information security risks that come prepackaged with the goods and services of certain overseas vendors."

http://reut.rs/2C14BO7

EUROPE

German court rules Facebook's use of personal data "illegal"

A German consumer rights group has said that a court had found Facebook's use of personal data to be illegal because the US social media platform did not adequately secure the informed consent of its users. The verdict, from a Berlin regional court, comes as big tech faces increasing scrutiny in Germany

over its handling of sensitive personal data that enables it to micro target online advertising. The Federation of German Consumer Organizations (VZVB) said that Facebook's default settings and some of its terms of service were in breach of consumer law, and that the court had found parts of the consent to data usage to be invalid.

https://ind.pn/2F1cP7y

UK government website offline after hack infects thousands more worldwide

More than 5,000 websites have been hacked to force visitors' computers to run software that mines a cryptocurrency similar to Bitcoin. Users loading the websites of the Information Commissioner's Office, the Student Loans Company, as well as the council websites for Manchester City, Camden, and Croydon—and even the homepage of the US Courts—had their computers' processing power hijacked by hackers. Malicious code for software known as "Coinhive," a program advertising itself as "A Crypto Miner for your Website" would start running in the background until the webpage is closed.

http://bit.ly/2H8bNqX

BT shares malware info with rival ISPs to combat cyber threat

BT is to share the malware data it gathers with its fellow Internet Service Providers (ISPs) in the United Kingdom. BT said it has become the first telecommunications provider in the world to start sharing information about malicious software and websites on a large scale with other ISPs. To help in this information sharing, the former UK incumbent has launched a collaborative online platform called the Malware Information Sharing Platform to allow fellow broadband providers to share threat intelligence data in a safe and secure manner.

http://bit.ly/2ErdJsV

RUSSIA

Russian military will not be allowed to use social networks

The Ministry of Defense has banned the military from using social networks, such as Facebook and its Russian counterparts. It was noted by the ministry that foreign resources have full access to the personal information posted there, and the publications of the Russian military are constantly being analyzed by foreign intelligence. Therefore, photographs and video materials attached to the terrain can "disrupt the combat mission."

http://bit.ly/2o3mORE

Russian military actively employs cyber forces in Syria

During the January 6 attack on the Russian military air base in Khmeimim in Syria, using flying drones, the Russian troops managed to reassert control over six drones out of total thirteen used, three of which were successfully landed on the ground. This indicates that Russian military contingent in Syria includes cyber forces, capable of executing cyberattacks and hacking enemy networks.

http://bit.ly/2BVw2si

Spain extradited Russian hacker Pyotr Levashov to the United States

Spain has transferred to US authorities the Russian hacker Pyotr Levashov, suspected of cybercrimes, the National Police said. It was noted that for several years Levashov "created a cybernetic infrastructure in the form of a botnet or a network of computers." In the United States, it is believed, that Levashov created a computer network such as the Kelihos botnet through which he "controlled hundreds of thousands of computers," spreading viruses, extorting, sending phishing emails, and making other spam attacks.

http://bit.ly/2H9TDVP

FBI dedicated to address Russian social media manipulation phenomenon

The FBI plans to alert US companies and the public about efforts by Russia or other nations to use disinformation and social media manipulation. The direction that the Federal Bureau of Investigation's "foreign influence" task force is heading could dramatically reshape the relationship between government and social media companies in order to address vulnerabilities that enabled Russia to meddle in the 2016 election.

https://bloom.bg/2BTyj7D

MIDDLE EAST

Saudi Arabia seeks to develop students' skills in cybersecurity

The Saudi prince's philanthropic foundation signed a memorandum of understanding with the Saudi Federation for Cyber Security and Programming to develop students' skills in cybersecurity and programming. Recently, Saudi Arabia signed agreements with Microsoft and Cisco systems to support local developers and innovators. The commercial companies will provide training equipment, access to tools, and licenses to their products.

http://bit.ly/2s8B68R

Lebanon's intelligence service accused of hacking Android phones

Lebanon's intelligence service has reportedly been accused of hacking into the smartphones of thousands of Android phone users and monitoring individuals' devices and data without consent. A report claims that Lebanon's General Directorate of General Security ran more than ten campaigns since 2012 aimed at Android users in twenty-one countries. The state-backed hackers tricked individuals into downloading fake versions of encrypted messaging apps, including Whatsapp and Telegram, giving hackers full access to their devices. The stolen data includes nearly half a million intercepted text messages, documents, photos, and audio. The main targets of the cyberattacks are government officials, military targets, utilities, and financial institutions.

http://bit.ly/2EvoiyX

Honeywell launches its first industrial cyber security center in the United Arab Emirates

Honeywell, a global technology and manufacturing leader, has launched its first industrial cyber security center at its Middle East headquarters in Dubai. The new center is a pioneering technology center with the ability to test and demonstrate process control network vulnerabilities and threats, train customers with real-time attack simulations, and provide advanced customer consultations. It aims to support the rapidly growing Middle East cybersecurity market and contains distributed control systems, a physical plant process, and the latest industrial cyber security software and solutions.

http://bit.ly/2o0L3AN

UAE company recruits Western intelligence services and works for the government

A small cyber security company in the UAE is recruiting executives who have worked for Western intelligence services and is heavily contracted with the government. Most of its work is with the UAE government and related entities and has included advising the federal cybersecurity agency, National Electronic Security Authority. This has helped the company, with ambitions to globally compete in the cyber sphere with IBM and Lockheed Martin, to double its revenue each year. It has hired executives who have worked at major international companies, such as Intel Corporation and BlackBerry, but also some with backgrounds in Western military and intelligence agencies, including the US National Security Agency.

http://reut.rs/2Evokqz

CHINA and APAC

Ravi Shankar Prasad: NIC should help India in becoming a low-cost cybersecurity hub

In the second national meeting of grassroots informatics, called "VIVID: Weaving a Digital India," Minister for Electronics and IT Dr. Ravi Shankar Prasad has asked the National Informatics Center (NIC) to take the lead in making India low-cost cybersecurity hub. The NIC was established in 1976 and

has since emerged as a prime builder of e-government applications at the grassroots level as well as a promoter of digital opportunity for sustainable development. The minister also highlighted that this initiative would supplement government efforts to make citizens literate in technology and expedite the process of making the digital economy reach the one-trillion-dollar mark in the next five years.

http://bit.ly/2o2takh

India, Oman agree to cooperate in security and defense.

During the visit of Prime Minister Narendra Modi to Oman, India and Oman agreed to enhance cooperation in law enforcement and cybersecurity, recognizing concerns regarding misuse of cyberspace as a medium to promote subversive and extremist ideologies. The two sides have mandated the concerned officials to hold discussions to identify avenues for cooperation.

http://bit.ly/2Cg8IkY

How Russian cyber meddling can inspire China

Kent Harrington, a former senior CIA analyst and national intelligence officer for East Asia, has said that Russia's cyber aggression has lessons for China's political warfare strategy. According to his analysis and observation of China's annual budget for internal security, maintaining domestic stability is a top priority for President Xi Jinping. China is also exploring how artificial intelligence and big data can be used to monitor everything from social media to credit card spending, and it plans to assign all citizens a social reliability rating to weed out potential troublemakers. Chinese cyber spies are also studying Russia's success. In addition to expanding China's cyber capabilities, President Xi Jingping has also been developing China's soft power through economic, social, cultural, and media initiatives.

http://bit.ly/2ElZR34

China's tough cyber rules raise risk of infiltration, US business group says

US-China Business Council says Beijing's demands on localizing data and revealing source codes raise the threat of security breaches. US President Donald Trump has also criticized China for its "unfair" trade action—such as forced technology transfers—and vowed a range of punitive responses, including tariffs, export quotas, and investment restrictions on Chinese firms' access to the US market. To comply with China's cybersecurity law, US online retailer Amazon sold part of its cloud business to its Chinese partner in November. And last month Apple announced it would set up a data center in Guizhou province and migrate information for China-based accounts to the center from the end of February. Provincial authorities will oversee the center.

http://bit.ly/2Ha3ELJ

Singapore's Ministry of Defense launches cyber scheme to bolster cyber defense capabilities

On February 12, Singapore's Ministry of Defense (MINDEF) signed its first work-learn memorandum of understanding with an educational institute where full-time national servicemen (NSF) are sent for academic upgrading while employed in an operational role. As part of ongoing efforts to strengthen cyber defense capabilities, MINDEF is launching the cyber NSF scheme to tap on cyber talents from the NSF pool. The plan aims to develop committed and skilled cyber NSFs to defend Singapore's military networks. Cyber NSFs will be deployed in a range of operational roles within the cyber domain. These functions are split into four broad areas: (1) cybersecurity monitoring, (2) threat assessment and response, (3) vulnerability audit and penetration testing, and (4) malware analysis and cyber forensics.

http://bit.ly/2CjQL56