Global Cyber Bi-Weekly Report by INSS June 1 2018

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

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

ISRAEL

"Fully prepared to face the threats"

Groups or individuals cyber threaten the State of Israel daily. Since the threat was first identified and defined, Israel has invested substantial resources in the war against cyber threats. The state-government executive arm is the National Cyber Directorate. The primary security resource is the cyber warfare operations center in Beer-Sheva or the national CERT. From the moment the cyber threats were identified, the Israeli government acted with determination toward the establishment of dedicated infrastructure that would fight cyberattacks. The National Cyber Directorate said that the Prime Minister had identified the significance of the threat at an early stage and is regarded as the patron of the National Cyber Directorate. As early as August 2011, the Israeli government sanctioned the establishment of the National Cyber Bureau, followed by the establishment of the Cyber Security Authority, and in late 2017, the government decided to merge the two individual organizations—the National Cyber Bureau and the Cyber Security Authority—into a single unit, the National Cyber Directorate. The Directorate is officially responsible for all aspects of cybersecurity in the civilian world, for policy consolidation, for the build-up of technological power and for operational cybersecurity. Yigal Unna, the head of the National Cyber Directorate, defined the nature of the threat at the CyberTech 2018 conference held in Tel-Aviv last January: "The cyber threats are growing more and more sinister. The cyber winter is already here, and Israel is no exception."

https://bit.ly/2shq7au

UNITED STATES

The bleak state of federal government cybersecurity

A recent White House Office of Management and Budget audit of federal government departments and agency cybersecurity preparedness showed poor results. OMB found 74 percent of the 96 US federal agencies to be either "at risk" or at "high risk." Most important, the report that is made public does not specify which agencies scored either "at risk" or "high risk." The OMB's vagueness in reporting seems to have caused more consternation than the findings as it is left to the reader to imagine which agencies are at high risk and which steps being taken to correct deficiencies.

https://bit.ly/2J2j1NI

Cyber mission force at full power: What now?

US Cyber Command, which was recently elevated to a combatant command, is now fully staffed and prepared for operations. Interestingly, the Cyber Command's focus will be on artificial intelligence and machine learning rather than relying on human review of data and imagery. This shift in focus will hopefully keep the US Cyber Command on par or above its adversary cyber forces.

https://bit.ly/2L9CJb3

Why the FBI says rebooting your router can weaken a global malware attack

CISCO warned recently that VPN Filter, malware connected to the Russian military, could infect as many as 500,000 routers worldwide. In light of this, the FBI recommends everyone reboot their home routers to their default settings and download the latest firmware. This simple act supposedly leaves VPN Filter at stage one not allowing it to spread into a network, which is necessary for it to download the second stage of the attack.

https://wapo.st/2L92x6T

EUROPE

Four EU cybersecurity organizations enhance cooperation

The European Union Agency for Network and Information Security (ENISA), the European Defense Agency (EDA), the European Cybercrime Center (EC3), and the Computer Emergency Response Team for the EU Institutions, Agencies, and Bodies (CERT-EU) signed a Memorandum of Understanding (MoU) to establish a cooperation framework between their organizations.

https://bit.ly/2IFprGv

Cyber security breaches survey 2018

New figures show large numbers of businesses and charities in the United Kingdom suffered at least one cyberattack in the past year. This report is a quantitative and qualitative survey of UK businesses, and it includes charities for the first time in 2018. The survey helps organizations to understand the nature and significance of the cybersecurity threats they face, and what others are doing to stay secure. It also supports the UK government to shape future policy in this area.

https://bit.ly/2xPTMgb

RUSSIA

Russia: The West tried to prevent Putin becoming president by using cyberattacks

According to the draft report of the Council of Federal Commission on Protection of State Sovereignty of Russia, the United States and a number of other western countries sought to prevent Vladimir Putin from being chosen as Russia's president in recent elections. According to the report, these efforts have been conducted since 2011. The commission also singled out ten main types of intervention during the last election campaign in Russia of which cyberattacks on resources of the Central Election Commission of Russia were most actively used.

http://bit.ly/2saQHSQ

New Russian defense control concept: Artificial Intelligence to control nuclear weapon tests by 2027

The Ministry of Defense of the Russian Federation will create an artificial intellectual system for controlling nuclear tests by 2027. The creation of an intellectual information system for controlling nuclear tests and geophysical conditions is planned for 2026–2027. It will become part of the overall development concept of the Special Control Service of the Ministry of Defense of the Russian Federation.

http://bit.ly/2KZ4rqV

Roskomnadzor blocked hundreds of Whatsapp IP addresses

The Federal Service for Supervision of Communications, Information Technology, and Mass Media blocked hundreds of Whatsapp IP addresses. Access to addresses was limited by a decision of the General Prosecutor's Office, which previously already blocked several million IP addresses of Google and Amazon hosting providers. It is assumed that blocking Whatsapp IP addresses is another attempt of Roskomnadzor to block the Telegram messenger app.

https://bit.ly/2xPqJJL

What lies behind Putin's renaming of the Ministry of Communication?

According to Russia Today news agency, Vladimir Putin's first decree since becoming Russia's President for another term was signing a decree about the structure of the new government of Russia, in which he renamed the Ministry of Communications as the Ministry of Digital Development, Communications, and Mass Communications of the Russian Federation.

http://bit.ly/2ISzJig

Russia to launch global underwater electronic surveillance system

According to Russian Izvestia news source, the Ministry of Defense of the Russian Federation began the deployment of global underwater electronic acoustic

surveillance system. According to the source, the system will be able to render entire regions of the world's oceans "transparent" for Russian military, detecting all ships, submarines, and even low flying aircraft. The system with the code name "Harmony" is based on the use of special robotized underwater modules.

http://bit.ly/2ksf5Li

Russian legislature officially does not recognize cryptocurrency as legal mean of payment

The Russian Federation's Parliament body (the State Duma) passed a bill on digital financial assets, in which such assets are not recognized as a legal means of payment in the territory of Russia. The document introduces definitions of digital financial assets, which include all types of cryptocurrency—including Bitcoin and Token-coin—as well as a new type of contract concluded in electronic form, the "smart contract." The draft law establishes that digital financial assets are not legal means of payment in Russia. It is noted that the document establishes the legal basis for carrying out activities that are aimed at creating a cryptocurrency.

http://bit.ly/2L1dh7x

CHINA and APAC

At Beijing security fair, an arms race for surveillance tech

The China International Exhibition on Police Equipment is something of a one-stop shop for China's police forces looking to arm up with the latest in "black tech." The fair underscores the extent to which China's security forces are using technology to monitor and punish behavior that runs counter to the ruling Communist Party. The Beijing-based Hisign Technology, present at the fair, said its desktop and portable phone scanners can retrieve even deleted data from over ninety mobile applications on smart phones, including overseas platforms like Facebook and Twitter. It also has the ability to get data from Apple Inc's iOS operating system, used in products like the widely popular iPhone. The Chinese-made XDH-CF-5600 scanner or "mobile phone sleuth" was also sold at the fair.

https://reut.rs/2JeHfHT

Scoping critical information infrastructure in China

At last month's national conference on cybersecurity and informatization, China's President Xi Jinping delivered the third speech on national cybersecurity meetings since 2014. Defining and protecting China's critical information infrastructure (CII) is a recurring issues mentioned at all three events. As the concept of information security evolved to become cybersecurity and a risk-based approach gained popularity in the global cyber community, the Ministry of Public Security vowed to upgrade the Administrative Measures for Information Security Multi-Level Protection Scheme (MLPS) to incorporate more dynamic cybersecurity safeguard elements for the protection of modern CII.

https://bit.ly/2LjJd7h

Australian Cyber Security Research Center appoints Rachael Falk as CEO

Former Telstra executive Rachael Falk is now heading the Australian Cyber Security Research Center as its new CEO, replacing interim CEO Dr Darrell Williamson. The Australian Cyber Security Research Center (CSRC) supports the Australian government's focus on cybersecurity as a national security priority. The CSRC is also not-for-profit organization devoted to promoting industry investment into cybersecurity research and development. The CSRC, which will be headquartered in Western Australia, will also deliver an Australia-wide approach to responding to cybercrime and cyber threats. It will also bring together government, industry, universities, and researchers to form a collaborative network that can tackle cybersecurity issues. The CSRC will work alongside the government's Cyber Security Growth Network (AustCyber). The CSRC's program will focus on two research themes, including cybersecurity in critical infrastructure and cybersecurity as a service.

https://bit.ly/2xCmRvz

CNL opens multi-million dollar innovation center for cyber security

Canada's national nuclear laboratory has opened its National Innovation Center for Cyber Security at Knowledge Park in Fredericton, New Brunswick. The multi-million dollar research facility represents a major addition to Canada's national cybersecurity capabilities, according to Canadian Nuclear Laboratories (CNL). CNL has identified cybersecurity research as one of seven strategic initiatives the company plans to pursue as part of its long-term strategy, a ten-year plan that will position the organization as a leader in nuclear science and technology. While there is a large commercial industry catering to the cybersecurity of business and information technology systems, the cybersecurity of industrial control systems has been widely overlooked, CNL said. Yet, this critical sector has shown vulnerabilities, with recent attacks on the Ukraine power grid in 2015 and 2016, a German steel mill in 2014, and the well-known Stuxnet attack in 2010. CNL can help customers find vulnerabilities in their security systems before they become an issue and without having to disrupt the operation of their facility.

https://bit.ly/2Lv5grG

Estonia completes cybersecurity training for Singapore's armed forces

The Estonian Ministry of Defence has delivered cybersecurity training and a cyber-range exercise to cyber defenders in Singapore's Ministry of Defence and to the Singapore Armed Forces (SAF), following the Memorandum of Understanding signed on January 19, 2018. The training took place at Singapore's Cyber Defense Test and Evaluation Center (CyTEC) and was delivered by the Estonian Defense Forces Cyber Range, which provides training opportunities from individual level training up to large-scale international exercises, said the Estonian Ministry of Defense.

https://bit.ly/2sO0ei1