Global Cyber Bi-Weekly Report by INSS April 15 2019

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

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

ISRAEL

Israel Aerospace Industries to help establish cyber defense academy in Brazil

ELTA Systems, leader of the Israeli Cyber Companies Consortium (IC3) and the Israeli Aviation Cyber Companies Consortium (IAC3), and the Brazilian National Confederation of Industries (CNI) are to collaborate on the establishment of a cyber defense academy in Brazil. ELTA Systems will work with SENAI, a non-profit organization administered by CNI, to create a Center of Excellence (CoE) for sharing cyber defense knowledge, education, and, in large, to promote cyber capacity build-up in Brazil. The aim is to strengthen and enable professionals to engage the "growing threats from hostile cyber activities and to establish the groundwork for relevant research and developments capabilities adapted for Brazilian needs" and to encourage forthcoming mutual cooperation between Israeli and Brazilian IP companies.

https://bit.ly/2VKnaMv

Cyber expert: Future elections will have even more cyber issues

According to editor-in-chief of Cybertech Magazine, Amir Rapaport, the "physical elections systems" remained unhindered during the recent 2019 Knesset elections. Credited to jointly coordinated efforts of multiple organizations, including Israel's Central Elections Committee, the National Cyber Directorate, and Israel Security Agency. Seemingly, the most relevant and notable example of election interference extends to the hacking of Blue and White party leader Benny Gantz's cell phone. Although no personal information from the device was published, the announcement of the hack posed a significant role, shifting Gantz to a defensive position. According to Rapaport, "Netanyahu capitalized on the issue by spreading fear of what personal information might be used by the hackers to extort Gantz." The

suspected utility of a network of bots or accounts by Likud Party supporters falsely advertised as nonpartisans to influence the public is not confirmed, although Rapaport states "there was no question that bots had been used by multiple parties during the election." Although, "bot social media accounts is not illegal on its own," Rapport stated an important element to bots in the future is to ensure their legitimate use, notably not to spread false information at any time period, not just during the "election cycle."

https://bit.ly/2KD5KQP

UNITED STATES

WikiLeaks' Assange arrested in London, faces US charge

Julian Assange, WikiLeaks founder, was granted sanctuary for nearly seven years by Ecuador, until recently when they revoked his political asylum "due to repeated violations to international conventions and daily-life protocols," resulting in his arrest and transfer from the Ecuadorian Embassy in London to court, commencing the "extradition battle." Assange faces multiple US charges connected to the publication of vast amounts of confidential state documents. A "strong standoff" is in motion between WikiLeaks and Ecuador's President Lenin Moreno, the former accusing the latter of revoking Assange's asylum due to their public accusations of Ecuador's "extensive spying operation" on him, as well as "allegations about an offshore bank account purportedly linked to Moreno's family and friends." Ecuador's Interior Minister Maria Paula Romo said "a close collaborator of WikiLeaks had traveled with former Foreign Minister Ricardo Patino this year to several countries—including Peru, Spain, and Venezuela—to try to undermine the Ecuadorian government. She did not identify the person."

https://bit.ly/2VKtx2g

Kirstjen Nielsen, a cyber-minded DHS chief, resigns

Kirstjen Nielsen resigned as head of the Department of Homeland Security (DHS) earlier this month, "ending the tenure of one of the most cybersecurity—focused secretaries the department has had in its 16-year existence." Nielsen was a proponent of implementing more consequences in cyberspace, demonstrating a tougher stance on foreign hackers. She was influential in getting the US Congress to codify DHS's Cybersecurity and

Infrastructure Security Agency Act into law (re-designating DHS's National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency with directorate resources and responsibilities transferred to the agency). It is speculated that she was "forced to step down" due to differences with the president over immigration policies. It was announced that "Kevin McAleenan, the current commissioner of Customs and Border Protection, will replace Nielsen on an acting basis."

https://bit.ly/2Ukin2K

US jury finds two Romanians guilty of stealing credit card info, infecting 400,000 computers

Romanian nationals, Bogdan Nicolescu and Radu Miclaus, were arrested in September 2016 in Romania and extradited to the United States in December of the same year. They recently were found guilty on 21 counts, including aggravated identity theft, wire fraud, and other charges related to money laundering and counterfeit charges. The malware infected an estimated 400,000 computers mainly in the United States. They used malware to extract credit card credentials and then sell that data on underground websites. The scheme also included "cryptocurrency mining, [and] robbing people of millions of dollars by duping them into making fraudulent purchases on supposed auction sites." This follows the "bust of a Romanian cybercrime ring," responsible for an "online auction scheme that defrauded Americans of millions of dollars." Subsequent of a four-year investigation led by former Homeland Security Secretary Kirstjen Nielsen, twenty people were indicted and an estimated dozen were extradited.

https://bit.ly/2GmJCG6

EUROPE

EU member states test their cybersecurity preparedness for fair and free 2019 EU elections

Earlier this month, in preparation for the May elections, the EU member states, European Parliament, European Commission, and the European Union Agency for Network and Information Security (ENISA) conducted an exercise to test the effectiveness of the EU responses and plans for prospective cybersecurity instances. The exercise is one of the measures utilized by the EU to ensure

states' capacity to "identify ways to prevent, detect, and mitigate cybersecurity incidents" and achieve unimpeded elections.

https://bit.ly/2UcpJp0

Gatwick drone attack possible inside job, say police

Between December 19 and 21, 2018, Gatwick, the second busiest airport in the United Kingdom, was closed for thirty-three hours, with an estimated 1,000 flights either delayed or canceled, affecting 140,000 travelers. Since the incident, the airport's chief operating officer, Chris Woodroofe stated "it was clear that the drone operators had a link into what was going on at the airport." Woodroofe added that "whoever was piloting the drone could either see what was happening on the runway, or was following the airport's actions by eavesdropping on radio or internet communications." Further supporting the "inside job" justification, according to Woodroofe, "whoever was responsible . . . specifically selected a drone which could not be seen by the DJI Aeroscope drone detection system that the airport was testing at the time." The perpetrator has yet to be found, and the investigation is still ongoing.

https://bbc.in/2UTPSxp

RUSSIA

US analysts: We will see more Russian cyber warfare in the near future

Cyber warfare has become an integral part of complex Russian warfare, in addition to hybrid and conventional strategies. According to US analysts, emboldened by successes in Syria and by its influencing of the 2016 American election, Russia will use high-tech disinformation campaigns combined with "limited" military actions as the cornerstones of a grand plan to divide the West and re-establish itself as a global power. The approach will combine Russia's infamous "hybrid warfare" method of using fake news stories and cyberattacks to achieve political goals.

https://bit.ly/2VKtx2g

Consequences of Russian "sovereign" internet regulations: foreigners are leaving

Owners of several large VPN services refused to comply with the requirement of the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) to connect to the Federal State Information System (FGIS) and block resources that are prohibited in Russia. In particular, this position was taken by TorGuard, the company that "completely removed the presence of physical servers in Russia." Roskomnadzor demanded from a dozen VPN services to connect to FGIS and start blocking resources prohibited in Russia. Notifications, in particular, were sent to NordVPN, Hide My Ass !, Hola VPN, Openvpn, VyprVPN, ExpressVPN, TorGuard, IPVanish, Kaspersky Secure Connection, and VPN Unlimited. For non-compliance with this requirement after the 30 days' deadline, the Russian authorities have threatened that the VPNs will be blocked.

https://bit.ly/2G6lhTC

Cybersecurity as main remedy against Russian possible aggression

After Russia proposed to integrate Belarus and Russia into common state, Belarusian authorities showed concern and approached their US connections, inviting them to hold NATO drills and bring American specialists in the field of monitoring social networks and controlling the internet. Belarus, spooked by Russian actions during the Ukrainian crisis, are considering all possible options, including cyber warfare, in their defense against their bigger neighbor, Russia.

https://bit.ly/2DVQQQf

APAC

Precision engineering firm Makino's new smart facility is able to nearly double machine production capacity

In 2016, Singapore launched "Precision Engineering Industry Transformation Map" (PE ITM), a joint partnership between industry and government agencies, intended to increase the "sector's output to $42 billion by 2020, from $32 billion in 2014." Part of the financial package, "industry-specific help," was

granted to companies such as Makino Asia, to enable its "digital transformation." The firm's latest investment is a $100 million smart facility, "expected to nearly double its machine production capacity through automation and data exchange technology." Additional benefits of the project is the investment in the workforce, including training and knowledge related to relevant "skills and mindset," according to Senior Minister of State for Trade and Industry Koh Poh Koon.

https://bit.ly/2Ii8KQA

Elbit to provide Guided Mortar Munitions to an Asia-Pacific country

Elbit Systems announced recently its contract of $30 million to supply STYLET to an unidentified country in Asia-Pacific. The "Precision-Guided Mortar Munition" is a multi-mode GPS/INS-guided 120mm GMM, with a range of 1000–8500m. STYLETs are highly accurate, increasing "tactical combat units and special forces operational effectiveness while reducing collateral damage." According to Yehuda Vered, general manager of Elbit Systems, "we see a growing demand for high-precision guided munitions that are also economically efficient." He also notes the company's improved position within the portfolio subsequent to the acquirement of IMI Systems. In reference to a previous article, the market research report compiled by Technavio, states that "APAC is anticipated to be the fastest-growing region in the SHORAD (short-range air defense) missile system market." Seemingly, the region is purchasing a number of varied defensive weapons, indicative of "the rise in the defense budget and subsequent development of defensive weapons."

https://bit.ly/2UG8H7N