Global Cyber Bi-Weekly Report by INSS Mars 15 2019

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

Contributors: Simon Tsipis, Anna Danilova, Gal Sapir, Michal Beit Halachmi, Robin Veldwijk

ISRAEL

Leading Israeli candidate for prime minister targeted by Iranian hackers

The campaign of Benny Gantz, a former Israeli military chief who is a leading challenger to Prime Minister Benjamin Netanyahu in his tight race for re-election says the candidate has been targeted by an Iranian hacking attack. Israeli media reported that the Shin Bet internal security service warned Gantz that Iranian intelligence hacked his cellphone, putting "his personal details and addresses in hostile hands." A statement from Gantz's campaign insinuated his opponents leaked the news to damage his political bid, saying the timing of the report just weeks before Israel's April 9 elections "raises important questions." A campaign official says the security breach happened several months ago, before Gantz entered politics. The official spoke on condition of anonymity because they were not authorized to talk to media.

https://abcn.ws/2TM7ZWi

Israeli cybersecurity company Cymulate raises $7.5 million

Israeli SaaS-based BAS platform cybersecurity company Cymulate today announced a $7.5 million Series A financing round. Cymulate will use the funding to expand US operations, add key leadership positions, and invest further in the research team to enhance the platform's functionality. Cymulate's BAS platform enables organizations to automatically assess their overall security posture, continuously validating that security measures and controls are working as expected. "The fast adoption of our platform by organizations optimizing their protection against attacks has enabled Cymulate to consistently surpass revenue and sales targets with triple growth which permits us now to focus on innovation and outreach. We've been very

strategic about the amount of funding we've raised in this round," said Cymulate cofounder and CEO Eyal Wachsman.

https://bit.ly/2O3IDNf

UNITED STATES

What's in the $9.6 billion cyber budget request?

The White House fiscal 2020 budget request for the DoD cyber activities marks an increase of $1.6 billion from last year, covering an array of cybersecurity and operational related components. Reflecting the former priority in hardware and software reforms, including research and development, to safeguard DoD's information and networks; with $5.4 billion designated toward advancing cybersecurity capabilities and $61.9 million toward improving their cloud ecosystems. Soliciting $3.7 billion in growing the capacity of the US Cyber Command, encompassing a mission force of 133 offensive, defensive and support teams. The requested funds are delegated to support the command's headquarters, infrastructure, offensive cyber operations, increased training, as well as research and development. The remaining half a billion dollars is ascribed to other capability boosting ventures, in addition to the other cyber developments pursued by the army, navy, and air force. Limited by justification, certain projects are noted to have dual "funding lines," as in the weapons system program referred to as Unified Platform; funded by the US Air Force in association with Cyber Command and the other services requesting $10 million, yet under a different line item, United Platform is itemized for $84.7 million.

https://bit.ly/2UDIFOs

Cyber Command's midterm election work included trips to Ukraine, Montenegro, and North Macedonia

On the heel of the partially published US cyber strategy (NSPM 13), posturing an approach in cyberspace as "persistent engagement" and "defending forward," has transpired in an increase of domestic inter-agency and foreign partnerships. Head of Cyber Command Gen. Paul Nakasone referenced an operation, a first for the cyber authority, during the recent House Armed Services Subcommittee hearing. In part of security preparations for the November 2018 US midterms, Cyber Command sent three defensive teams to

Ukraine, Montenegro, and North Macedonia; the former exposed hostile Russian cyber campaigns, while the latter two are associated with NATO, a threat to Russian influence. The operation was aimed to collaborate in network defense, as well as support, learn, and gain information about adversaries and their capabilities, among other elements, particularly Russia. According to Burke Wilson, the deputy assistant secretary of defense for cyber policy, defensive cyber operations were conducted as well.

https://bit.ly/2HqLW0K

EUROPE

UK cybersecurity efforts criticized by audit office

The UK government has been told there are "failings" in the way it is planning to protect the critical infrastructure from cyberattacks. The warning came in a National Audit Office (NAO) assessment of the UK national cyber defense plan. The government is increasingly worried that these essential sectors will be targeted by foreign states seeking to disrupt UK life.

https://bbc.in/2T9QRof

NATO picks BlackBerry's encrypted voice technology to secure calls

BlackBerry has announced that the NATO Communications and Information (NCI) Agency has awarded a contract for BlackBerry's SecuSUITE for Government to encrypt the conversations of its technology and cyber leaders wherever they communicate—in the workplace, at home, or traveling abroad. The NCI Agency helps NATO's twenty-nine member-nations communicate securely and work together in smarter ways. It acquires, deploys, and defends communication systems for NATO's political decision makers and command centers, working on the frontlines against cyber attacks.

https://bit.ly/2OeuDkd

RUSSIA

An inside peek into Russia's biggest IT "trolling factory"

A Russian "trolling factory" named "Concord, situated in Saint Petersburg, in Olgino district, which is suspected by the US authorities and Muller's investigation as the source of US presidential election meddling, costs one million dollar a month. It has hundreds of PC stations and employs bloggers, paid commentators, translators, specialists working with Live Journal, Facebook, Twitter, Instagram, Telegram, and many other forums and social networks, analysts, and computer scientists. The goal of the biggest IT factory is to directly influence world media, targeting social opinion on almost any subject considered essential for the Kremlin's political and social goals, from the US and domestic elections to military interventions outside Russia. The Concord factory is managed by an ambiguous figure, Evgeny Prigojin, also known as "Putin's Chef." "Social opinion engineering" is defined by the Kremlin as one of the most important field of local and foreign politics. Due to Russia's huge population stratum, social opinion seems significant for Putin's regime survival. Among other things, the IT "trolling" factory deals with "mitigating" consequences of terrorist attacks in Russia (including the Volgograd attacks in December 2013), lowering the scale of military losses in foreign interventions (including in Syria), upgrading Putin's rating, and suppressing the opposition.

http://bit.ly/2XQSHOt

Russian "sovereign internet" is a countermeasure against US Cybersecurity Strategy

Russian Parliament, the State Duma, adopted in the first reading a bill on the stability of the "Runet" – Russia's "sovereign" internet, the development of which was decreed by President Putin's administration. According to the law, all domain names and site addresses will be authorized and controlled by the Federal Service for Supervision of Communications, Information Technology and Mass Media—"Roskomnadzor." According to the special Duma committee, the draft law "was prepared taking into account the aggressive nature of the US National Cybersecurity Strategy adopted in September 2018."

http://bit.ly/2O0DcPn

Russian law prohibits internet usage for its soldiers

Russian parliament votes to ban army personnel from sharing information on the internet, following a Russian journalist's investigations and multiple leaks regarding the locations and losses of Russian military personnel around the world, particularly during the war in Ukraine and in Syria. According to Reuters, the draft legislation adopted by the regime was to conceal Moscow's clandestine role in foreign conflicts. Draft legislation proposes banning servicemen and reserve troops from posting anything online that would allow outsiders to glean their whereabouts or role in the military.

https://reut.rs/2VVKnLq

The head of US Cyber Command: Russia will go as far as it feels allowed

The head of the National Security Agency and US Cyber Command, Admiral Mike Rogers told lawmakers during Congress hearings that Russia is definitely about to intervene in the 2020 US elections. "The Intelligence Community concluded last year that Russian actors, with the knowledge of senior decision makers, employed influence operations to interfere with the US presidential election in 2016," Rogers said. According to Admiral Rogers, Putin will only stop this malicious meddling when confronted by a "determined opposition" to it. And thus far, as the admiral testified, Putin has felt nothing of that.

https://cnn.it/2NYA7PE

Estonia is at the forefront of countering Russia's cyber aggression

Estonia is considered the first member state of the European Union that was cyberattacked by Russia in 2007 and seems to be the leading state to successfully counter Russia in cyberspace. The country has recruited a few hundred volunteer hackers to respond to the kinds of electronic attacks that have flummoxed the United States and other countries in recent years. These civilians have security clearances and the training to handle such attacks. The IT militia of amateur workers, economists, lawyers, and other white-hat types are grouped in the city of Tartu, about sixty-five miles from the Russian border, and in the capital, Tallinn. The volunteers are preparing to defend against sustained digital attacks that could cause mass service outages at

hospitals, banks, and military bases, and with other critical operations, including voting systems. Officially, the team is part of Estonia's 26,000-strong national guard. French authorities say they have been inspired by the Estonian system, and Latvia set up a similar unit a few years ago. Through a partnership with the US Department of Defense, the Maryland National Guard's digital squads have trained with Estonian forces, and the head of Michigan's Cyber Civilian Corps is planning to visit Tallinn later this year.

https://bloom.bg/2J8MvOh

Foreign software companies leaving Russian market

American software developer Splunk decided to stop selling its products and services to Russian companies. Splunk is a major developer of machine data analysis and operational activities. The company was founded in 2003, its headquarters are located in San Francisco, and its offices are represented in twelve countries. The press service of the developer did not comment on the decision to leave Russian market.

http://bit.ly/2TARrQL

APAC

North Korea hackers are targeting critical infrastructure

A new report, issued by McAfee, indicates that North Korean hackers are continuing their efforts to target US infrastructures, including oil, government departments, and nearly eighty businesses ever since September 2017. The hacking attempts were first spotted during heated times between the United States and North Korea and continues as talks and two summits were already held between Donald Trump and Kim Jung Un. MacAfee claims it is working with at least one government entity but refused to disclose the name. It is believed that the hacking operation has numerous technical links to the Lazarus Group. North Korea is believed to run nearly 200 hacking groups worldwide, including from Namibia, which has claimed to cut all ties with North Korea. The operations primarily target Germany, Turkey, and the United Kingdom, as well as the United States. North Korea has become a major cyber threat in recent years, but unlike others, is focusing its energy on cash, as per John Demers, assistant attorney general for national security at the US Justice Department.

https://goo.gl/fe6aYW

UN report links North Korea hackers to theft of $571 million from Crypto currency exchanges

A UN panel of experts, which is comprised of UN-appointed analysts and reports to a committee of the UN Security Council, published a report that entails North Korea's attempts to circumvent sanctions using multiple methods, including hacking crypto currency exchanges. North Korea breached at least five crypto currency exchanges in Asia between January 2017 and September 2018, causing $571 million dollars in losses, most of it from the January 2018 hack to CoinCheck in Japan, and $81 million dollars theft in 2016, from a Bangladesh bank.

Using cryptocurrency exchanges is especially useful for evading sanctions, as it is hard to trace the digital trail. Hugh Griffiths, who heads the panel of UN experts, states that the report highlights the amount of money involved and scope of operations taken, as well as the ability to breach bank security, which is extremely worrisome and raises broader cyber security questions.

https://goo.gl/SQDfxD

China's Huawei opened a new transparency center in Brussels

The center opened a day after Huawei filed a legal suit against the US government, alleging that it is banning all federal agencies from using its products. The United States has long warned against Huawei, claiming that their equipment is being potentially compromised by the Chinese government. According to Associated Press, the cybersecurity lab "will be a platform where government agencies, technical experts, industry associations, and standards organizations can collaborate on cybersecurity." Other Huawei centers are located in Germany and the United Kingdom, and Huawei is interested in opening a security testing center in Poland, which might be problematic due to a recent arrest of a Huawei employee on espionage allegations.

https://goo.gl/ecAoNS

Japan to establish the first Asia-Pacific alliance for cybersecurity

The alliance will be composed of twenty-seven countries and organizations, including members of the ASEAN Regional Forum, which is comprised of Japan, the United States, the European Union, Australia, India, China, and Russia, as well as the ten countries in the Association of Southeast Asian Nations. The first forum meeting is scheduled for August, when the first step of forming a joint cybersecurity office will be discussed. Members will use the alliance to share laws, policies, and strategies, as well as to conduct joint research on defending critical infrastructure, protection methods against hacks, and joint exercises to fight cyberattacks. It would also be the first multilateral cybersecurity alliance that includes China, which showed interest in participating in such a forum. However, having China and Russia in the forum might prove to be problematic due to their high-profile cybersecurity activities against other countries. Japan expects to start measures on cybersecurity attacks ahead of the August forum, which will discuss creation of common cybersecurity guidelines and mechanisms to protect power supply and crucial infrastructure.

https://goo.gl/S9KCRZ