Global Cyber Bi-Weekly Report by INSS May 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

IDF cyber warriors thwart major ISIS aviation terror attack

The Israel Defense Force (IDF)'s Unit 8200 played a large role in thwarting a major Islamic State terrorist attack, which aimed to bring down a civilian airliner headed from Sydney to Abu Dhabi this past summer. In cooperation with Israel's intelligence community, the Unit 8200 provided exclusive intelligence that they had gathered on an attack that was being planned. The intelligence led to the arrest of the suspects who were in the advanced stages of executing the plot. "The thwarting of the attack led to the saving of the lives of dozens of innocent people and demonstrated that Unit 8200 is a player in the intelligence war against Islamic State," stated an IDF officer. Unit 8200 is regarded as Israel's equivalent of the National Security Agency in the United States. According to Australian officials, the ISIS-inspired attack against an Etihad Airways flight from Sydney to Abu Dhabi was thwarted in July. While Islamic State's territorial "caliphate" may have crumbled, the IDF does not believe that the threat posed by the terrorist group is over, as terrorists have moved from Syria and Iraq to places like Egypt's restive Sinai Peninsula, which borders Israel. Unit 8200 soldiers were also responsible for thwarting a recent Iranian hacking attack against private and public organizations in Israel. The attack was thwarted in cooperation with the defense division of the IDF's telecommunications department and by the "close monitoring of the operations of the Iranian network and the early identification of attempts to attack Israel," the IDF said.

https://bit.ly/2HAN5mX

Israel accounts for second largest number of cybersecurity deals globally

A new report compiled by the New York data firm CB Insights shows that Israel accounted for the second largest number of cybersecurity deals

globally, behind the United States and ahead of the United Kingdom. The report shows that Israel accounted for 7 percent of the cybersecurity global deal share in the years 2013–2017, still way behind the United States, which accounted for 69 percent of the global deal share, but higher than the United Kingdom, which accounted for 6 percent of the pie. The report selects 29 cybersecurity startups—which it calls cyber defenders—who are early-to-mid-stage high-momentum companies pioneering technology with the potential to transform cybersecurity. Out of these, six are Israeli firms, ranking the so-called Startup Nation with the second highest concentration of cyber defenders, after the United States.

https://bit.ly/2r6vFU9

British banks target Israeli security technology

According to a report by the British Israel Communications and Research Center (Bicom), which conducts research on Israel and the Middle East, British banks are working with former Israeli military cybersecurity specialists to secure the banking infrastructure against cyber attacks, as London seeks to boost its position as a global financial center in the run up to Brexit. Israeli cybersecurity companies are providing security expertise to at least three of the top four UK banks. The introduction of EU regulations requiring authentication of digital financial transactions—known as the European Revised Payment Service Directive—has led to closer cooperation between UK companies and Israeli firms that specialize in biometric and other forms of authentication. HSBC opened a cyber hub in Tel Aviv last year. Barclays and Royal Bank of Scotland have also set up research and development (R&D) centers in the country to tap into Israeli technology, including cyber security, biometric authentication, data analytics, and payment technology. Last year, Aviva Insurance, BT, Goldman Sachs, RBS, Visa, and others hosted Israeli cyber security startups for a series of events in London.

https://bit.ly/2vP8JhQ

UNITED STATES

Tech groups push “Geneva Convention” to help foil cyberattacks.

According to the Financial Times, a US-led group of technology companies are pledging that they will not help governments "mount attacks on innocent citizens and enterprises." Brad Smith, Microsoft's president and chief legal officer, is leading the charge. Backers include HP, Facebook, Cisco, Nokia, ABB, and ARM. Notably, Apple, Amazon, and Google have not given their support. Smith says his aim is "to keep pushing the countries of the world for a new digital Geneva Convention." According to IISS and CSIS cyber experts, there seems to be much consternation in these broad pledges and how the use and definition of the term "innocent" can really be put into practice.

https://on.ft.com/2JXGAbd

DHS to roll out national cybersecurity strategy in mid-May

The Department of Homeland Security (DHS) plans to roll out its new cybersecurity strategy in the next two weeks. A cyber strategy from DHS has been long in the waiting and the 2018 strategy is said by current DHS Secretary to be more forceful than in the past. Speaking at a conference, she hinted that DHS will be more forceful in responding to nation-state actors as well as in stepping up a recruiting drive. Competition from the private sector has been putting DHS at a disadvantage. To remedy this the department will appeal to applicants' sense of patriotism and mission.

https://bit.ly/2KmrOuY

United States and Britain blame Russia for a global cyberattack

Washington and London are warning of the possibility of a Russian attack on routers and networking equipment in order to target government agencies, businesses, and critical infrastructure. They point to the recent NotPetya attack in Ukraine during 2017 targeting the country's power grid. The White House's cybersecurity coordinator went on to say "when we see malicious cyber activity, be it from the Kremlin or other malicious nation-state actors, we're going to push back." This notes an overt change in posture and some attribute this to private sector criticism of the US government having been too passive and tight-lipped with the public in warning of possible cyberattacks.

https://reut.rs/2vUinQ0

EUROPE

Tech firms could face new EU regulations over fake news

Brussels may threaten social media companies with regulation unless they move urgently to tackle fake news and Cambridge Analytica-style use of personal data before the European elections in 2019. The EU security commissioner, Julian King, said "short-term, concrete" plans need to be in place before the elections, when voters in twenty-seven EU member states will elect members of the European Parliament. The Cambridge Analytica affair had "served to highlight how important [the issue] is," he told the Guardian. Based on King's ideas, social media companies would sign a voluntary code of conduct to prevent the "misuse of platforms to pump out misleading information."

https://bit.ly/2K9TjHZ

Nearly half of UK manufacturers hit by cyberattacks

Some 48% percent of UK manufacturers admit they have at some time been subject to a cybersecurity incident, with half of them suffering financial loss or disruption to business as a result, according to the report published by EEF, the manufacturers' organization, in partnership with AIG, the insurance firm, and the Royal United Services Institute (RUSI). While 91 percent of the nearly 170 UK manufacturing businesses polled are investing in digital technologies, 35 percent consider that cyber vulnerability is inhibiting them from doing so fully. More than four in ten manufacturers do not believe they have access to sufficient information to confidently assess their specific risk, and 45 percent are not confident they are prepared with the right tools for the job. According to the report, a "worryingly large" 12 percent of manufacturers surveyed have no process measures in place at all to mitigate against the threat, and only 62 percent of respondents said they train staff in cybersecurity, while 34 percent said they do not offer cybersecurity training, and 4 percent said they did not know.

https://bit.ly/2FiQ3GM

NATO cyber defenders tested at world's largest cyber drill

NATO cyber experts will test and train their ability to defend against cyberattacks in the largest international live-fire cyber defense exercise,

Locked Shields (April 23–27). A team of thirty from the NATO Communications and Information Agency (NCIA) will be taking part in the week-long event, alongside a thousand national experts from around thirty nations. The competition has been organized annually by the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) based in Tallinn, Estonia, since 2010. Locked Shields is an opportunity for cyber defenders to test the protection of their IT systems and critical infrastructure in a safe environment, under realistic challenges by world-class opponents.

https://bit.ly/2KnCEAF

Islamic State web media targeted in EU-led attack

Cyber specialists in various European countries, Canada, and the United States targeted online sites, including the Amaq News Agency, considered the main Islamic State mouthpiece. Europol coordinated a "simultaneous multinational takedown" of Islamic State media, seizing digital evidence and servers. Islamic State jihadists may now be identified. The Islamic State broadcasts in several languages. The EU members involved in Europol's operation on April 25–26 were Belgium, Bulgaria, France, the Netherlands, Romania, and the United Kingdom.

https://bbc.in/2HWDHJx

Cybercrime website behind four million attacks taken down

A British and Dutch-led operation on April 25 brought down a website linked to more than four million cyberattacks around the world, with banking giants among the victims, Britain's National Crime Agency (NCA) said. "Authorities in five countries including the Netherlands, Serbia, Croatia and Canada, with support from Police Scotland and Europol, targeted six members of the crime group behind webstresser.org," the NCA said in a statement. Cybercriminals used the website's services, which could be rented for as little as US $14.99 (£19.93), to launch distributed denial of service (DDOS) attacks, which swamp targets with traffic and disable their IT systems. British police searched an address in Bradford in Northern England and seized a number of items, while Dutch police, with assistance from Germany and the United States, seized servers and took down the website.

https://bit.ly/2r7oo74

RUSSIA

British intelligence: Russia about to attack our infrastructure

According to the British Sunday Times, referring to sources in the security agencies, British intelligence agencies are ready to attack Russian computer networks in response to possible "aggressive" actions of Moscow in cyberspace. According to the source, British cyber experts have already "taken positions" in computer networks in Russia. London expects cyberattacks on the country's key infrastructure and particularly on the healthcare system.

http://bit.ly/2KjoCQA

Is the Kremlin about to launch "The Great Firewall Of Russia"?

After Russia blocked the Telegram messenger service in accordance with its court's decision, along with Amazon's and Google IP addresses, which were used by the Telegram messenger, according to Head of Roskomnadzor Alexander Zharov, to bypass the Russian blocking systems, information has surfaced about Russia's "Great Fire Wall" project under development, the analogue of China's internet filter. Dmitry Peskov, the press secretary of the Russian president said that the Kremlin is not considering to create an internet filtering system in Russia.

http://bit.ly/2Fl8AlJ

The hidden US-Russian war for hackers

According to Russia's RIA Novosti, US intelligence agencies, in particular the NSA, are trying to recruit Russian hackers who have been arrested by the US authorities or extradited to the United States due to cybercrimes. Until now, eighteen Russian hackers have been arrested by US authorities outside of Russia, including two whom Russia managed to bring back. The latest arrest of Russian hacker is of Alexander Vinnik, who is now in Greece and whom both powers are trying to get.

http://bit.ly/2vO8eEF

MIDDLE EAST

Iran Cyber Security Group hacks Harvard's Undergraduate Council website

The Harvard's Undergraduate Council's website was briefly hacked by a group calling itself the "Iran Cyber Security Group." During the hack—which lasted for at least half an hour—visitors to the website encountered a cartoon of President Donald Trump being punched in the chin by an individual whose face was not depicted but who wore a wristband with the colors of the Iranian flag: green, white, and red. The hack appeared to affect only the Council's homepage, which is hosted on a domain of the Faculty of Arts and Sciences, according to its URL.

https://bit.ly/2vZ4X5u

Islamic State propaganda websites attacked by international security services

The propaganda machine of Islamic State has been hit by an unprecedented multinational cyber campaign, but the terrorist group is still managing to reach thousands of its followers. British security services were involved in the assault targeting websites hosting its flagship Amaq "news agency," alongside EU, US, and Canadian allies. Europol said the group's ability to broadcast and publicize terrorist material has been "compromised" by cooperation with both internet service providers and cyberattacks.

https://ind.pn/2HHACJS

Popular UAE hospital website cloned, doctors targeted in new scam

In the latest job scam in the UAE, a group of fraudsters have sent fake appointment letters to job aspirants in India, offering them huge salaries and perks. To add authenticity to their letters, the fraudsters have created a fake website in the name of Thumbay Hospital and mirrored the original website into their URL. The fake website was created on April 20, 2018, and is registered with an Amsterdam address and phone number, which are not traceable.

https://bit.ly/2jftXw3

CHINA and APAC

Australian ministers to meet with Google, Apple in the name of cybersecurity

The Australian government has sent cybersecurity representatives to the United States this week, hoping to strengthen the cyber alliance between both countries. Minister for Law Enforcement and Cyber Security Angus Taylor, Commonwealth Cyber Coordinator Alastair MacGibbon, and Australian Federal Police Assistant Commissioner Neil Gaughan are expected to meet with US government counterparts and senior officials in Washington, including the Department of Homeland Security and the Federal Bureau of Investigation. The trio will also meet with representatives from PayPal, Twitter, Apple, and Google to "encourage deeper cooperation with governments to address challenges faced by law enforcement."

https://zd.net/2w0xaJf

Pyongyang in frame as cyberattack hits home

Cyber researchers from McAfee, the computer security company, say at least three "systems" in Australia were infected last month by what they believe was an attack by North Korea's state-sponsored hacking unit, Hidden Cobra. McAfee was unable to say what data had been stolen in the attack. Cybersecurity expert Greg Austin of the Australian Defence Force Academy's campus at the University of NSW said the attack could be unsettling for US president Trump's North Korea summit.

http://bit.ly/2vW3Svl

DHS cybersecurity program adds South Korean cybersecurity agency to threat indicator partnership

The Automated Indicator Sharing (AIS) system of the Department of Homeland Security (DHS) added the Korea Internet and Security Agency as a new partner to its shared exchange. US Senators Mazie Hirono (D-Hawaii) and Cory Gardner (R-CO) previously wrote to the DHS in support of adding South

Korea to the system, over North Korean fears. The AIS works to protect both governmental and private interests, working toward a cyber-secure community at large. Thus far, thirty-three federal and 175 non-federal entities are connected to the system. Among these, thirteen states are connected to AIS.

http://bit.ly/2JD9lZL