Global Cyber Bi-Weekly Report by INSS 15 July 2019

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

Contributors: Simon Tsipis, Robin Veldwijk, Thomas Abma, Donal Byrne

ISRAEL

TV: Israel intelligence foiled fifty Islamic State and Iranian attacks in twenty countries

The Mossad intelligence agency and the Military Intelligence Directorate have prevented dozens of Islamic State terror group and Iran-sponsored attacks in various countries around the world by providing local authorities with key information, according to a recent television report by Channel 12. It thwarted fifty attacks in twenty countries over the past three years. Prime Minister Benjamin Netanyahu said that Israel had used cyber intelligence to help foil "major" terror attacks planned by the Islamic State terror group and others in "dozens" of countries, like Turkey. At a cybersecurity conference, Netanyahu explained that Israel helped foil an attack by Islamic State on an Etihad Airways flight from Sydney to Abu Dhabi and alerted Australian officials, helping thwart an explosion in the air. A senior Israeli official said that the Mossad was responsible for providing British authorities with information that helped foil the Iran-backed efforts by Hezbollah to stockpile explosives in London in 2015. According to a report by the Daily Telegraph, Hezbollah operations in Thailand, Cyprus, and New York were also thwarted.
https://bit.ly/2JoYpBK

Israeli cybersecurity company enSilo raises $23 million

Israel cybersecurity company enSilo, founded by Roy Katmor, Udi Yavo, Tomer Bitton, and Ido Kelson, announced the completion of a $23 million financing round led by Rembrandt Venture Partners. The company raised $32 million in its first financing round in 2016¬–2017, in which OG Tech Ventures and Viola

also took park. enSilo says that the purpose of the financing round is to "continue extending the platform's proven prevention, detection, thwarting, and response capabilities." Together with the financing round, the company announced "annual growth of over 250% in revenue, expansion of its strategic partners, including new territories in Central and South America and in Asia." enSilo has 86 employees, including 53 in Israel. The company plans to hire 10–20 more research and development personnel in the coming year.
https://bit.ly/2XLuI6T

Israeli firm presents its anti-terror tech to high-profile US delegation

Israeli cybersecurity company Cobwebs, based in Herzliya, was founded five years ago by Omri Timianker, Udi Levy, and Shay Attias, all alumni of special IDF units, and specializes in gathering intelligence data with a security orientation from all over the internet. The company last week hosted a delegation of members of the US House, led by Representative Ted Deutch, D-Fla., who is the chairman of the US House Middle East and North Africa Subcommittee; Congressman Gus Bilirakis, a member of the Committee of Energy and Commerce; Congressman Henry Cuellar, a member of the Committee on Appropriations; and Congressman Randy Weber, a member of the US government Committee on Science, Space, and Technology. "We saw many gaps in the cyber intelligence arena," Levy told the Jerusalem Post, explaining that the company has developed technology for gathering open source intelligence by using big data, artificial intelligence, and machine learning to help clients "work faster with what they have." With just one click, authorities can identify connections between criminals or terrorists which would otherwise be missed. Cobwebs supplies its products to law enforcement agencies, government agencies, as well as financial agencies around the world for use in criminal investigations of human trafficking, drug smuggling, arms dealing, counterterrorism, computer fraud, and money laundering. It has around 80 employees with offices in New York, Singapore, and Israel.

https://bit.ly/2LReK3H

UNITED STATES

Are Congress and the White House on a collision course over cyber?

A little over a year ago, the National Security Presidential Memorandum (NSPM) 13 came into effect; allowing the president to override certain procedures to "delegate to delegate certain cyber authorities to the Secretary of Defense for particular missions." The legislative branch has requested to review "documents governing cyber operations," and has yet to receive them from the executive branch. Rep. Jim Langevin, chairman of the House Intelligence and Emerging Threats and Capabilities Subcommittee, said earlier this summer that "congress has a vital role to play in ensuring any offensive cyber operations do not inadvertently undermine that stability and reflect our commitments to responsible state behavior in this new domain." An additional occurrence was the recent objection by the executive branch concerning "a provision in the pending House version of the annual National Defense Authorization Act requiring the Secretary of Defense to notify Congress within 15 days anytime leaders delegate specific authorities for military cyber operations."
http://bit.ly/2JySA4L

Mystery of NSA leak lingers as stolen document case winds up

Former contractor for the NSA, Harold Martin who was arrested on the suspicion of stealing "government hacking tools," is due to go to trial at the end of the month. The theft has been described as "breathtaking in its scale," and was leaked by the group referred to the Shadow Brokers, whose identity remains unknown until today. Martin apparently stole thousands of pages of secret documents over a two-decade career in national security, most recently with the NSA. He pleaded guilty to a single count of willful retention of national defense information and faces a nine-year prison sentence under a

plea deal. It is still uncertain whether Martin and the Shadow Brokers are connected, and to what extent, if any, were Russia or North Korea involved or if they benefitted from the leaked data.
http://bit.ly/2JzI796

Engineer took US locomotive manufacturer's source code to China, prosecutors say

The Department of Justice recently released an indictment that has been sealed since December 2017, involving former engineer Xudong "William" Yao, who has been charged with nine accounts related to the embezzlement of intellectual property. It is suggested that Yao stole more than 3,000 files, including "source code, technical documents and other sensitive data" from his former employer, a locomotive manufacturer in Illinois. Yao apparently had accepted a job in China at a company that made automotive telematics service systems half a year before he was fired from the company in Illinois. When he returned to China in July of 2015, prosecutors alleged that he had nine complete copies of the US company's control system source code and the systems specifications that explained how the control system source code worked.
http://bit.ly/2NWkY51

EUROPE

European Union struggles to pick next cybersecurity chief

Europe's cybersecurity authorities are struggling to select the next chief of the EU cybersecurity agency. The EU Agency for cybersecurity recently received more powers under the new Cyber Act, a landmark regulation that came into force at the end of last month. In the coming years, the agency will be tasked with improving the protection of internet-connected devices and boosting the security of 5G telecom networks, among other things, across the European Union. A selection procedure that should have ended in March is still ongoing, however, due to differences between member states and given the sensitivity

of the role. The new executive director needs the votes of two-thirds of EU capitals, and must then appear before the European Parliament's industry committee. The vote will occur next week.
https://politi.co/32qpQm5

British Airways hit with record £183 million fine for new EU data breach

The UK government has announced its intention to fine British Airways for breaches that compromised the personal and financial data of hundreds of thousands of its customers under the EU's new General Data Protection Regulations (GDPR). The penalties will incur fines of a proposed £183 million for British Airways. The move gives clarity on how EU regulators will determine whether the security measures that a company undertakes are considered "adequate" enough within the European Union. While this fine is the largest to date since the establishment of the new GDPR regulations, British Airways has confirmed that it intends to appeal the fine.
https://on.ft.com/2LSsRpM

RUSSIA

The US drone downed by Iran apparently was hunting the "Red October"

The downing of a US drone last month, which belonged to the US Navy Cyberwarfare Department, and which had surveillance and cyber strike capabilities, might have had other intentions in the region. An op ed. published in Forbes argues that the mission was to disable the computer systems used to control Iranian rocket and missile launches, but it was targeted against Russian systems, located in Iran. According to the analysis, "the critical dependency on space, resulting in new cyber risks that disproportionately affects mission assurance" for both Russia and the United States compel them to hunt for one another's cyber capabilities.

According to a report by Chatham House, the two nations are likely to have set out to compromise the satellite networks used by each other and their allies as Russia prioritizes electronic warfare, cyberattacks, and superiority within the electromagnetic battlespace, and both nations both focus on preventing adversarial satellite-based communications systems from impacting their operational effectiveness. According to the report, this particular type of attack has been seriously debated in the Pentagon, since the US military has relied on satellite battlefield communications for generations. This reliance, however, has expanded to include missile defenses, unmanned weapons guidance, target acquisition, and the advanced ISR capabilities embedded in command and control programs.
http://bit.ly/2SeaKLU

US cybersecurity community got "cold feet" vis-à-vis Russia

According to the US cybersecurity community, today's cyber-arms race has proven far easier to accelerate than to slow down. But security experts tend to agree, at least, that there is one way not to prevent a cyberwar—by launching a preemptive or disproportionate cyberattack on an opponent's civilian infrastructure. As the Trump administration increasingly beats its "cyberwar drum," some former national security officials and analysts warn that even threatening that sort of attack could do far more to escalate a coming cyberwar than to deter it. As was recently reported, the US Cyber Command has penetrated more deeply than ever before into Russian electric utilities, planting malware potentially capable of disrupting the grid, perhaps as a retaliatory measure meant to deter further cyberattacks by the country's hackers. However, judging by Russia's response, news of the grid-hacking campaign may have already had the opposite effect: The Kremlin warned that the intrusions could escalate into a cyberwar between the two countries.

Officials, such as White House national security adviser John Bolton, have for months hinted at a more aggressive approach to cyber operations against US adversaries. However, former White House cybersecurity officials are rather cautious against such cyberwar hawkishness. Tom Bossert, who served as

White House homeland security advisor and the president's most senior cybersecurity-focused official, until April of last year, warns that "I want to make sure we don't end up in an escalatory cyber exchange where we lose more than they do." Former secretary of defense Ash Carter said, "if you're doused in gasoline, don't start a match-throwing contest." The Obama administration's cybersecurity coordinator J. Michael Daniel echoed that warning, arguing that if the Trump administration and Cyber Command are indeed taking a more offensive approach to penetrating Russia's grid, then they are doing so without truly knowing the potential consequences. Georgetown University professor Ben Buchanan calls this dangerous ambiguity in his recent book, "the cybersecurity dilemma." Rob M. Lee, who once led industrial control systems threat intelligence at the National Security Agency, points to a recent Cyber Command attack on the Internet Research Agency troll farm in St. Petersburg as an example of a more measured and targeted operation, destroying only the servers of the Kremlin-linked disinformation operation, without causing any of the collateral damage inherent in an attack on a power grid. "There are plenty of ways to go after valid military targets and cause some level of discomfort, or just messaging, that would be far more acceptable than jumping straight to civilian infrastructure." "It will blow back," Lee says, "But I don't oppose it because it will blow back. I oppose it because it's not ethical. I don't think it is in keeping with the kind of country we want to be."
http://bit.ly/2XI2WZ0

Cyber cold war between the United States and Russia escalating rapidly

The cyber cold war between the United States and Russia continues to heat up, with one accusing the other for having either hacked or are seeking to hack each other's power grids. On both sides, each country, either directly or through state-sponsored hackers, allegedly are attempting to insert malware into networks that, if triggered, could bring down part or all of the other country's electricity network. A report published recently claimed that

Xenotime, the Russian group behind the Triton malware, which attacked oil and gas assets in the Middle East in 2017, is now probing US power grids. The security firm Dragos has claimed that since late 2018, the group began probing the networks of electric utility organizations in the United States and in the Asia-Pacific region.
http://bit.ly/2XJUbxg

MIDDLE EAST

Saudi Arabia rolls out first batch of cybersecurity graduates

Cybersecurity and defense company Trend Micro announced the first Saudi national graduation from its local Graduate Academy for Cyber Security Program. Following the two-year program, ten Saudi citizens have graduated and have already found career replacement in the Trend Micro ecosystem. "Saudi Arabia's organizations need smart, technically proficient, and business-savvy Saudi nationals to lead the Digital Economy," said Dr. Moataz bin Ali, vice president of Trend Micro Middle East and North Africa.
http://bit.ly/32namzg

Forcepoint survey finds Middle East companies do not use behavioral analytics to stop breaches

Research from global cybersecurity Forcepoint found that organizations fail to use behavioral analytics to identify and prevent cyberattacks. Forcepoint points out that this is believed to be a crucial step toward effectively preventing breaches. Even though 85 percent agree that analyzing behavioral analytics is a critical component of cyber strategy, only 54 percent reportedly have acted on it. This type of data reveals insights into the behavior of consumers on platforms and applications and analysis can help make them more secure.
http://bit.ly/2XN6MLk

Bahrain, UK governments partner to pilot global AI guidelines

The governments of Bahrain have announced it will partner with the UK government to pilot new guidelines for artificial intelligence (AI) investment in the public sector. A statement said AI has huge potential to streamline and transform service delivery for governments but due to lack of understanding and concerns over its complexity, public institutions are often wary of adopting it. This spurred the World Economic Forum to bring together governments, businesses, start-ups, and civil society to tackle this issue.
http://bit.ly/2YUgZqW

APAC

Second Chinese cybersecurity center opens in Brussels raises suspicion

ZTE, a Chinese telecommunications company has opened a cybersecurity lab in Brussels, aimed to boost transparency. This comes just four months after Huawei, telecoms equipment rival, did the same and came under suspicion for doing so. The United States and some of its allies criticized Huawei, as they believe the equipment could be used by Beijing to spy on customers if deployed in 5G networks, which are beginning to be built around the world. Huawei, the world's largest producer of telecoms network gear, has been blacklisted by the US government. This means that US companies need special approval to export products to the Chinese company. ZTE, which is not blacklisted, said its new cyber lab would allow customers, regulators, and other stakeholders to review its source code and documents and to carry out software testing to simulate hacking attacks. ZTE almost went out of business last year when US suppliers were banned from supplying it with components in a trade row with Iran. However, the ban was lifted in June 2018 after it paid a $1 billion fine.
http://bit.ly/2Gesli1

Coding classes for primary pupils to be introduced next year in Singapore

The Singapore government is taking steps to ensure that its citizens will have the fundamental skills and attributes to thrive in the digital age and to consider a career in cybersecurity. An expanded "Code For Fun" program will be piloted this year at some schools across Singapore with the hope that it will be implemented nationwide by next year. Introduced as an optional program in 2014, it aims to help students learn computational thinking through basic coding while emerging technologies such as artificial intelligence will also be covered. The Singapore Cyber Youth Program (SG Cyber Youth) will encompass students from both secondary to tertiary level education. Students will benefit from exposure to relevant knowledge and skills, and it is hoped it will encourage younger people to consider a career in the area of cybersecurity.

http://bit.ly/2JwcVYq