Global Cyber Bi-Weekly Report by INSS June 15 2019

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

Contributors: Simon Tsipis, Thomas Abma

ISRAEL

Israel moD, Lockheed Martin sign F-35 maintenance agreement

The Production and Procurement Department of the Israel Ministry of Defense and Lockheed Martin Israel recently have signed a first-of-its-kind F-35 aircraft maintenance agreement. Lockheed was awarded the contract worth over NIS 150 million, in which the "aircraft manufacturer will provide expansive maintenance services [and operate….the advanced training center for the F-35 aircraft at Nevatim Airbase] to the Israeli Air Force," for the next five years with the possibility to extend for another five. The service support extends to the full mission simulator (FMS) and Autonomic Logistics Information System (ALIS). Twenty-five Israeli employees will be employed by Lockheed for the project as well.

https://bit.ly/2IgPaTI

IHLS Accelerator Startup: Revolutionizing passenger and cargo management

Israeli startup RubiQ has created "a ground-breaking resource allocation solution" for human transportation and cargo delivery platforms. The AI solution streamlines and improves dialogue between airline companies and passengers due to delays and cancellations. In the context of military, the "real-time logistics solution to the problem of grounded military trucks or aircraft, when cargo and staff must be transferred to other locations," is amended. It is estimated to cost airlines and passengers $60 billion a year due to "flight disruptions, like overbookings, cancellations, or delays," and is only

heightened by the current "resolution process . . . manual management." Aircules, an all-in-one platform, automates and optimizes the entire operation from end-to-end. It utilizes "AI to pre-emptively identify flights at risk of disruption and communicate with affected passengers through their virtual assistant [via a web application] to notify them accordingly and offer personalized flight alternatives, thus eliminating the need for passengers to check their flight status and interact with the airline representatives at the check-in counter. All passengers are then automatically accommodated by the allocation engine, reducing the inefficient distribution of accommodation fees and accelerating the airline response times."
https://bit.ly/2wXeffY

UNITED STATES

Watchdog finds ten "critical" IT security risks in the government

Out of the $90 billion budget the government allocates to information technology, 80 percent is used to maintain its legacy IT systems, according to the recent Government Accountability Office (GAO) report. The ten identified systems contributing to "security risks, unmet mission needs, staffing issues and increased costs," need modernization and include the Department of Defense, Department of Education, Department of Health and Human Services, Department of Homeland Security, Department of Interior, and Department of Treasury. The unnamed systems "cost approximately $337 million for their agencies to maintain." Based on a 2018 risk assessment on the Department of Homeland Security's Legacy system, uncovered "249 reported vulnerabilities, of which 168 were considered high or critical risk to the network." Not all the agencies have developed modernization plans.
https://bit.ly/2wXeAPM

Raytheon, United Technologies announce mega merger

Raytheon and United Technologies, the respective Massachusetts and Connecticut-based companies will merge, becoming Raytheon Technologies Corporation, with an expected annual revenue of about $74 billion. Aimed at creating an "aerospace and defense powerhouse," valued at an estimated $121 billion, this merger is recognized as one of the largest-ever in the aerospace and defense sector. According to CNN, both companies "are worth about $166 billion in market value now." According to the deal, United Technologies shareholders would own 57 percent of the combined company, with Raytheon shareholders owning the rest. In a press release, it was stated that the company will "expand technology and R&D capabilities to deliver innovative and cost-effective solutions aligned with customer priorities and the national defense strategies" of the United States and its allies.
https://bit.ly/2XQTePY

Salesforce to acquire Tableau for $15.7 billion in all-stock deal

Saleforce, the customer-relationship management (CRM) behemoth, recently agreed to purchase the big data company Tableau Software for $15.7 billion in an all-stock deal. This purchase marks the biggest acquisition in the company's history. The acquisition will increase Salesforce's fiscal revenue in 2020 by $300–400 million. Tableau is an analytics platform, based out of Seattle, Washington, and has more than 86,000 customers, including Verizon, Southwest Airlines, Schneider Electric, and Netflix. Salesforce CEO Marc Benioff stated, "Tableau helps people see and understand data, and Salesforce helps people engage and understand customers. It's truly the best of both worlds for our customers."
https://bit.ly/2ZmFnRE

EUROPE

Europe prepares to thwart net threat

Kalashnikov KUB, also referred as a "suicide drone," is the latest Russian drone technology. It is "designed to be launched covertly and explode when within

target range." Its capabilities seemingly are combined with the Orlan-10 UAV (unmanned aerial vehicle), although it is considered to be more of a serious threat. The drones fly in threes—the first providing reconnaissance, the second carrying electronic warfare systems to jam NATO communications, and the third transmits intelligence information to a control center. Justin Bronk, airpower and technology expert with the Royal United Services Institute, stated that "these drones routinely carry electronic warfare payloads. Russia could release a cluster of nine Orlan drones to carry out electronic warfare, such as jamming NATO communications. It did this effectively in Syria and Ukraine." Such capabilities challenge NATO and pose a high risk in the "swarm tactic" being utilized effectively in the invasion of Ukraine, to disrupt NATO communications as a prelude to a ground incursion. Recently specialists from Belgium, Netherlands, France, Germany, Italy, Norway, and Spain "simulated exercises at the European Air Group headquarters at Buckinghamshire; focused on a hybrid Russian attack in the Baltic involving cyber and disinformation offensives and a drone swarm attack."
https://bit.ly/2IMwBWl

The EU Cybersecurity Act: A new era dawns on ENISA

In efforts to strengthen the European Union Agency for Network and Information Security (ENISA), the EU Cybersecurity Act, or regulation (EU) 2019/881 will enter into force at the end of the month, binding and applicable in all EU member states. The provisions related to penalties and the role of the judicial arm will enter into force June 2021. ENISA will be known as the EU Agency for Cybersecurity and will receive a permanent mandate and will have more resources and responsibilities to support cybersecurity initiations across the European Union. The Cyber Act will build on creating a secure environment within the European Union, by implementing the first EU-wide cybersecurity certification framework for businesses so that they can achieve cybersecurity certification for their information and communications technology (ICT) products, processes, and services. The Cybersecurity Act

aligns with the EU General Data Protection Regulation and the EU Network and Information Security Directive (NIS Directive).

https://bit.ly/2ZrjgJO

https://bit.ly/2ZsCSxm

https://bit.ly/2KOXuvy

Elbit nears $200 million German aircraft protection deal

Elbit, the Israeli defense electronics company, is in progressive talks to sell DIRCM (Directional Infrared Counter Measures), an aircraft protection systems to the German Air Force for about $200 million. Elbit aims to equip about 53 A400M transport aircrafts of the Bundeswehr's fleet, according to the German Federal Ministry of Defense. The DIRCM system directs infrared beams at the shoulder-launched missile and diverts it from its path toward the aircraft it is targeting. In efforts to expand in the German market, Elbit opened an office in Berlin in April 2018 and has since worked with German defense forces on developing capabilities, DIRCM being one of them, along with DIEHL BGT Defense. Other advances include, supplying tactical radio systems as well as advanced electro-optic systems for infantry soldiers. Elbit has been growing in the German and other key European markets, including in the UK Military Flight Training System, the Benelux Smart Vest program, the Swiss Unmanned Aircraft Systems program. It also provided self-protection systems for NATO's A330 fleet and an unnamed European country with an array of electronic warfare and signal intelligence systems.

https://bit.ly/2FbSr4y

https://bit.ly/2wXLQXg

https://bit.ly/2IjgcK8

RUSSIA

A "smoking gun" for Russia's cyber-manipulation with GPS signals is revealed

Norway's Defense Ministry has electronic proof that Russian forces disrupted global positioning system (GPS) signals during recent NATO military drills and has demanded an explanation from its eastern neighbor. In November 2018, both Finland and Norway said that Russia may have intentionally disrupted GPS signals before and during Western military exercises, which also affected the navigation of civilian air traffic in the Arctic, but now they have the solid proof of it. Although Finland is a non-NATO partner, it also participated in last year's NATO's largest exercise in decades—involving forces from 31 countries in an area stretching from the Baltic Sea to Iceland. Apparently, this is not the first cyber-military attack that these states have experienced from its neighbor.

https://reut.rs/2OzV8R5

The "great fusion" of Russian IT-business and Russian military intelligence

A Russian internet tycoon and IT businessman, Aleksej Gubarev, is apparently connected to the Russian intelligence, including the GRU military service, and has provided them with internet infrastructure and cyber tools for hacking outside Russia. According to the FBI, Gubarev, who runs companies in Europe and the United States providing cut-rate internet services, is connected to Russia's interference in the 2016 presidential election and the complicity of the Trump campaign. According to the Dossier media source, Gubarev's companies used "botnets and porn traffic to transmit viruses, plant bugs, steal data, and conduct 'altering operations' against the Democratic Party leadership in 2016."

https://nyti.ms/2IbCc9I

Russia's "hybrid warfare" strategy employs cyberattacks

According to an assessment by the United State and its ally, the new Russian geopolitical strategy will include an over-extended usage of "hybrid warfare" in which cyberattacks take a leading role. According to the analysts, Russia—emboldened by the successes in Syria and in influencing the 2016 American

elections—will further use high-tech hacking and disinformation tools and tactics to further undermine Western positions, whereas the main goal is to divide the West and reestablish itself as a global force. Central to the broader plan is dividing the United States and its NATO allies in order to prevent a strong, coherent international response to further aggression in Eastern Europe, the Middle East, and in cyberspace.
http://bit.ly/2KLsbSm

MIDDLE EAST

Insider breaches remain serious issue for businesses, including UAE and Middle East according to new report

In its 2019 "Privileged Access Threat Report," BeyondTrust explores the visibility, control, and management that IT organizations have over employees, contractors, and third-party vendors with privileged access to their IT networks. The report reveals that 64 percent of organizations believe they have likely had a direct or indirect breach due to misused or abused employee access in the last twelve months, while 62 percent believe they have had a breach due to compromised vendor access. The report claims that only 28 percent of Middle East businesses worry about employees downloading data onto a memory stick, compared to 42 percent in the Asia-Pacific region.
http://bit.ly/2XA7LiU

Saudi company invests in UK agricultural tech firm

The Saudi Agricultural and Livestock Investment Company (SALIC) announced a round of investments in the London-based Hummingbird Technologies, valued at £7 million. The agtech (agricultural technology) company "uses imagery and data analytics from satellite, drone, plane, and robot technology to boost agricultural practices." SALIC's managing director, Khaled Al-Aboodi, stated the company "aims to be a world-class agribusiness investment company focusing on food security," while the company intends to make

sizable, meaningful, and scalable investments" by investing in new agricultural technology projects.
http://bit.ly/2R550Uc

Bahrain to take legal action against users following critical Twitter accounts

Bahrain's Ministry of Interior said in a tweet on Thursday that "those who follow inciting accounts that promote sedition and circulate their posts will be held legally accountable." This move marks a heightening of control of the small kingdom over social media. Last month, the Bahrain News Agency reported that Bahrain is in the process of drafting a bill that would include penalties for the misuse of social media. The Chairman of the Council of Representatives' Committee for Foreign Affairs, Defense and National Security, Mohammed Ibrahim Al Sisiharms stated that the government plans to deal firmly with the "misuse of social media," which is seen as disturbing "community peace," and as weakening Bahrain's national unity. A draft law will also focus on defamation, insult, spreading rumors, and infringing on individuals, bodies, entities, and state institutions.
http://bit.ly/2WyiyIW

APAC

China to strongly retaliate against US cyberattacks

A report published by China's National CNCERT (Computer Network Emergency Response Technical Team) states that many of the cyberattacks on Chinese networks in 2018 came from within the United States. The report warns that China is prepared to retaliate by launching full-scale cyberattacks on the United States. CNCERT says that the previous year witnessed over 3,607 Chinese websites being infected by trojan viruses from 3,325 IP addresses based in the United States—an increase of 43 percent when compared to the statistics of 2017. The Chinese seem to assume that US intelligence agencies implant viruses and hack information from the terminals

of Chinese customers to steal data from applications and websites, specifically those connected to military and government organizations.
https://bit.ly/2IilzJG

Vietnam cyber threat: Government-linked hackers ramping up attacks

The threat intelligence firm IntSights has published a threat brief on Vietnan's growing offensive cyber capabilities. The threat brief is authored by Charity Wright, a cyber threat intelligence analyst and former NSA offensive Asia Analyst. Whihle the current cyber threats have been primarily a response to economic issues, the new ones are in response to internal political issues. A new cybersecurity law came into effect at the beginning of 2019 and requires companies, like Google and Facebook who have opened offices in Vietnam, to store local user data in Vietnam, and to hand over personal information to the government on demand. The law also allows censorship, which has consequentially led to the migration of youth to the dark web. "As Vietnamese authorities attempt to strengthen their grip via censorship, they drive more and more Vietnamese citizens to the dark web for access to unfiltered content," says Charity Wright.
https://bit.ly/2WEhEKZ