UNCLASSIFIED

INSS
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
Cyber Warfare Program
Executive Cyber Intelligence
Bi-Weekly Report by INSS-CSFI
THE CYBER SECURITY FORUM INITIATIVE

Executive Cyber Intelligence Bi-Weekly Report by INSS-CSFI

October 1st, 2014

This document was prepared by The Institute for National Security Studies (INSS) – Israel and The Cyber Security Forum Initiative (CSFI) – USA to create better cyber situational awareness (Cyber SA) of the nature and scope of threats and hazards to national security worldwide in the domains of cyberspace and open source intelligence. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities, and follow-on measures. This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted. These materials, including copyrighted materials, are intended for "fair use" as permitted under Title 17, Section 107 of the United States Code ("The Copyright Law"). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner. Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: dcoi@inss.org.il.

CSFI and the INSS would like to thank the Cyber Intelligence Analysts who worked on collecting and summarizing this report.

ISRAEL

Israel establishing new national cyber defense authority

Prime Minister Netanyahu declared the establishment of a new national cyber defense authority in conjunction with the Israeli National Cyber Bureau (INCB). They will be responsible for proactive protection of Israel civilian cyber space, linking the civilian and security spheres, coordinating between leading experts, and leading long-term strategic defense thinking. Dr. Eviatar Matania, Head of the INCB, was instructed to designate the creation and was asked by the Prime Minister to introduce a proposal for the Israeli Knesset in 60 days.

More cyber revelations post Operation Protective Edge

More information has been revealed on cyber-attacks that occurred during Operation Protective Edge. The revelations came from the Israeli Navy. “What we have seen during Operation Protective Edge was an increase in attacks, when you can’t always identify the source,” a source inside the Israeli Navy cyber unit ISPC (Information Systems, Processing, and Computing), stated to news site Mako. The classified source explained there had been attempts to hit the Navy’s C4I systems and disabe them. The source added: “In Protective Edge we have seen a rise of the cyber camping. It is not an army that you can identify. It starts with a lone hacker that sees a pro-Palestinian challenge in facing the Israeli Navy or IDF, and it ends with National States. We felt the intensification of the attempts for cyber warfare during the op, but on the other hand, it was contained. We were prepared and knew how to deal with it.”

USA

USCYBERCOM to recruit 6,000 cyber professionals and create 133 teams across the country

The US Cyber Command (USCYBERCOM) intends to recruit 6,000 cyber experts and create 133 teams of soldiers and civilians from military branches to assist the Pentagon in defending the US national infrastructure. Currently, the agency to be charged with protecting the US against cyber threats remains unclear; however, USCYBERCOM hopes to create a more focused authority. Previously, all branches of military performed their own cyber security measures. This comes after House Committee Chairman Mike Rogers (R-Michigan) expressed an interest in having the US adopt an offensive strategy in cyberspace that would require not only the Pentagon, but intelligence agencies and law enforcement to develop protocols for offensive cyber measures. Rogers explained, "We haven’t coordinated that policy. We have disparate levels of cyber offensive capability across the federal government. …Some are fantastic, some not so good, and then [there are] some in the middle.”

RUSSIA

Russia wants to disconnect the ".ru" from interconnected web

Taking full state control on the ".ru" domain and Internet as a whole on Russian territory is part of the Kremlin's recent agenda. The Kremlin is considering radical plans to unplug Russia from the global Internet in the event of a serious military confrontation or big anti-government protests on homeland, according to Russian officials. President Vladimir Putin will discuss with the Security Council what steps

Moscow might take to disconnect Russian citizens from the web "in an emergency." The goal would be to strengthen Russia's sovereignty in cyberspace.

ARAB COUNTRIES

ISIS and Al-Qaida looking for cyber Caliphate to launch attacks on US

Middle Eastern jihadists, Islamic State (IS) and al-Qaeda, are planning a joint massive cyber-attack on the US. ISIS publicized openly their plans to establish a "cyber caliphate" protected by jihadist developed encryption software in which they hope to use in creating a catastrophic cyber-attack through hacking and viruses deployed against the US and the West. The jihadists have already developed their own constant developing software to protect their own communications against Western agencies. In addition, they are attempting to add to their numbers to boost their capabilities by using social media for recruitment and calling on militant-minded specialists to join them. The targets are the websites of US government agencies, banks, energy companies, and transport systems. IS's efforts are led by a British hacker, Junaid Hussein alias Abu Hussain Al Britani, who is a key recruiter calling upon computer experts to join IS. He joined IS over a year ago by arriving into Syria and has previously led a group of teenage British hackers known as Team Poison.

New Qatari Cyber Law threatens freedom

Qatar has been urged to revoke sections of a new cybercrime law stating it threatens freedom of expression within the Gulf state. The Committee to Protect Journalists (CPJ) warned that the broad language of the new Anti-Cybercrime Law could be used to restrict freedom of the press and could potentially jail journalists. According to CPJ, "This law is ostensibly to stop cybercrime, but at least two articles will severely restrict freedom of expression, which is not a crime… The Qatari authorities should repeal all articles in this law which curb press freedom." CPJ is referring to Article 6 that stipulates up to three years' imprisonment and a fine of 500,000 riyals for setting up or managing a website that spreads "false news aimed at jeopardizing state security." CPJ also pointed to Article 8 of the law, which adheres to a jail term of up to three years and a fine of 100,000 riyals ($27,500) for any "violation of social values or publishing news, pictures, audio or video recordings that are related to individuals' private life and family, even if true."

CHINA and APAC

Singapore organized 23rd GovernmentWare infocom security exhibition

The theme this year of Singapore's 23rd GovernmentWare infocom security seminar and exhibition was "Strengthening the Cyber Security Ecosystem." Public and private sectors convened to learn about the latest challenges in IT security. As large-scale cybersecurity breaches continue to make headlines around the world, Singapore is taking a proactive approach to counter cyber threats by growing its infocom security talent pool and strengthening its monitoring and incident response capabilities. Minister of Communications and Information, Dr. Yaacob Ibrahim stated a Monitoring and Operations Control Centre (MOCC) will be established to provide the government with a full suite of capabilities to guard against security threats and respond to them in a timely manner. The MOCC will complement the Cyber-Watch Centre (CWC), which will be upgraded by January 2015 to strengthen the government’s detection and analytical capabilities.

Multinational cyber security drills
Twelve Asia-Pacific countries participated in performing cyber security incident responses at the 2014 ASEAN Computer Emergency Response Team (CERTS) Incident Drills (ACID) in Hanoi. Cyber security agencies of the countries included Vietnam, Australia, China, Japan, India, and Singapore. The exercise role-played hackers exploiting and attacking a hole in an Indian website's server, while others were analyzing and identifying intended lessons from cooperation in cyber security incident responses.

Australia's Department of Finance drafts cyber security clauses defining service providers’ responsibilities when managing cyber security risks
The Australian Department of Finance is inviting feedback from the IT industry about the draft of cyber security clauses. Department of Finance Assistant Secretary, Mundi Tomlinson, wrote that the cyber security clauses are designed to dDfine service providers’ and contractors’ responsibilities in order to manage cyber security risks, provide clear contract arrangements for safeguarding government data, and increase the visibility of cyber security incidents.

The draft clause states the contractor must do all things that a “reasonable and prudent entity” would do to ensure that customer data is protected at all times from unauthorized access or use by a third party. If a data breach occurs, the contractor must notify the customer in writing. It must also contact the Australian Cyber Security Centre, or other cyber security organisation such as AusCERT, as required by the customer.

EUROPE

UK to launch real-time cyber threat alert system for banks in 2015
A new real-time cyber threats system will be deployed in the UK bank industry next year to help financial institutions fight against cyber security threats, fraud, and financial crime. According to the UK Financial Crime Alerts Service (FCAS), this real-time intelligence system will assist in countering terrorist financing, money laundering, bribery, corruption, online crime, fraud, and other emerging cyber risks for banks. This intelligence information will come from different agencies such as the National Crime Agency, the MI5, etc. This new Intelligence system will be developed by the company BAE systems Applied Intelligence and should be operational for the beginning of 2015. It will provide intelligence to help banks react more efficiently and to be able to handle threats. Moreover, the system should be able to help them to spot emerging threats by performing proactive intelligence. After the major attack of JP Morgan, the UK is strengthening its financial cyber security industry by using intelligence systems to prevent financial systems from cyber-attacks and network infiltrations.

French Information Systems Security Agency strengthening its cyber defense
The French Information Systems Security Agency has recently decided to strengthen its cyber defense. From the 30th of September until the 3rd of October, a cyber defense exercise was exercised, which allows the military to test their ability to

manage a crisis in a fictional international context. The French General Staff of the Army explained that the DEFNET exercise is the first of its kind and particularly innovative because of its global nature, "It can drive our specialized forces from the lowest level to the highest level. DEFNET 2014 marks the beginning of a new process of operational readiness." The Ministry of Defence declared that several scenarios would be imagined, such as a defense contractor undergoing cyber-attacks or hacktivists who are threatening military networks, with soldiers acting as fake journalists to test the nerves of those responsible for countering these cyber-attacks. In Europe, France is one of the biggest countries, yet it is still far behind the UK in terms of cyber defense capabilities. France started to improve its cyber defense and capabilities in 2009 with the creation of the National Agency for the Information Systems Security (ANSSI). Today, the French cyber defense is much stronger but still needs improvement within the private sector, including recruiting more cyber specialist in private high tech companies, banks, telecoms, and defense industries to counter the large scale of cyber-attacks they are facing.