UNCLASSIFIED



Executive Cyber Intelligence Bi-Weekly Report by INSS-CSFI

July 15th, 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: inssdcoi@gmail.com.

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

ISRAEL

Operation Protective Edge hits ~~the~~ cyber realm

As Operation Edge rage~~d~~s on, hackers have increased their attempts to breach Israel, and while most of the attacks were unsuccessful, some hackers did succeed in their attempts. The IDF blog and spokesman T~~t~~witter account was hacked by the Syrian Electronic Army (SEA). The SEA defaced the blog by posting a message ~~against~~ opposing Israel's alleged crimes against the Palestinians and Syria. On the IDF blog and Twitter, SEA published a fake tweet claiming: "possible nuclear leak in Dimona, after 2 rockets would have hit the nuclear facility in Dimona." ~~-~~ It was revealed that hackers used an APT (advance persistent threat) attack and phishing mails to get access into the account. Another popular website hacked was the Haaretz website. In response to these ~~cyber-attacks~~cyber-attacks, the Israeli hacker team Israel Elite Force is beginning their own response attack called #OpIsraelRetaliate taking place on July 17th~~17.7~~. In an article published on pc.co.il, Professor Yitzhak Ben Yisrael claims that since the start of the Operation there was ~~a raise~~an increase of 900% in cyber-attacks against Israel. Before the Operation began, there had been 100,000 a day, yet during the Operation the number has risen to over a million.

Operation Protective Edge in ~~the~~ cyber industry

The Israeli cyber industry also reacted to the O~~o~~peration, and a number of applications were created to deal with the situation. One application developed presented a red color system alarm for iPhone, Android, and other chrome browsers that no matter where a person is, ~~they~~ he/she will be able to know if there is a siren going off in ~~their~~ his/her region or in other places. Another development created was an app for finding a bomb shelter, basement, or shelter ~~in your~~within close region.

U~~.~~S~~.~~A

U.S. engaged in talks with China regarding ~~their~~ cyber spying activity

Senior U.S. officials, who participated in meetings with the Chinese last week, stated either side did not raise the case of the hacking into the Office of Personnel Management. The Chinese, angered by the indictment in May of five members of the People's Liberation Army on charges of cyber espionage, refused a request by the Americans to restart a joint cyber working group. China suspended the work of the group that brought together American and Chinese negotiators to discuss cyber issues and has complained that the National Security Agency documents made public by Edward Snowden showed the United States had used cyber espionage to gain economic advantage.

DOD~~'s working to bolster~~bolstering cyber security resources within civilian and military networks ~~of individual countries~~

The DoD's cyberwarriors are working to bolster cyber security resources within civilian and military networks of individual countries, which are defined by the Department of Defense as those countries who are particularly more susceptible to cyber-~~-~~attacks~~-~~. Acting D~~d~~eputy Assistant Secretary of Defense for Cyber Policy, U.S. Army Maj. Gen. John Davis, said several international allied countries faced a "significant impact... ~~. . .~~ [or] existing threats" of active cyber-attacks particularly those in the Pacific, which are at risk of cyber-attacks from China and Russia.

Additionally, General Davis said U.S. allies in the Middle East and Asia-Pacific regions were the primary focus of U.S.-led cyber defense efforts. The U.S. government has claimed those nations are responsible for offensive cyber operations against American allies, as well as attempted intrusions into U.S. networks. At the same time, DoD officials are working to improve NATO's ability to respond to attacks against nations within the alliance. They're are ~~working~~ collaborating in a slew of cyber working groups to determine joint approaches and strategies to defend against attacks. NATO allies created a "Cyber Incident Response Center~~,~~" meant to act as a reporting and coordination hub for cyber operations in the case of an attack against NATO or its members.

AFRICA

South Africa's cyber crime increases

A recent report compiled by McAfee, found cyber-crime is having a significant economic impact on South Africa. The impact is costing the country over R5.8 billion each year – a situation believed to continually be getting worse. DDoS attacks are seen as a key concern by 66% of South African organizations. This is higher than the global average, which is 58%. It also reveals that while the majority of South African organizations do have a DDoS defense plan in place, only 20% believe they have sufficient resources to counteract such an attack.

Cyber sSecurity iIssues tTake cCentere sStage at 5th Kenya Internet Governance Forum

The 5th annual Kenya Internet Governance Forum held in the beginning of July at Strathmore University forcused on c~~C~~yber s~~S~~ecurity issues ~~take center stage at the 5th annual Kenya Internet governance forum held in the beginning of July at Strathmore University~~. The theme of the forum was ''Connecting Counties for Enhanced Multi-S~~s~~takeholder Internet Governance.'' The key points raised focused on the emerging legal concerns and challenges relating to cyber security. According to the Kenya Cyber Security Strategy released in February 2014, criminal organizations and hacktivists from all over the world are - and will continue to be - ~~to~~ exploiting ICT vulnerabilities in Kenya as the country matures into an Information Society, adding that the country will face an increasingly evolving cyber threat landscape. Currently, Kenya ranks fifth in terms of hacking globally.

CHINA and APAC

~~A~~ Nnew Australian Center for Cyber Security

A new cyber security center has been launched at the University of New South Wales in Canberra. ~~-~~ACCS brings together the largest group of cyber security researchers in the country~~,~~ and will be located at UNSW Canberra at the Australian Defence Force Academy. The ACCS intends to be a unique, interdisciplinary cyber security research and teaching center. UNSW Canberra prides itself on bringing together leading edge research with practical real-world applications. "ACCS is a perfect example of how university research can support the business community and government," says Rector of UNSW Canberra, Professor Michael Frater. ACCS draws on the skills of some of the best cyber security experts in the country serving as an expert in legal,

policy, and technical domains. “UNSW applies this leadership through research; teaching; and engagement with the government, Defence, and business community,” says Director of ACCS, Professor Jill Slay.

North Korea ~~is~~ expaending ~~it~~ cyber power

In the last few years, North Korea has expanded its cyber power. Two years ago the cyber war unit of the Korean People's Army had around 3,000 cyber soldiers and today has about 5,900. The country has doubled its cyber capability. The North Korean cyber unit seems to operate under the control of the General Bureau of Reconnaissance, which includes around 1,200 hackers. According to the Seoul-based Yonhap News Agency, the country has established new cyber bases in China and other countries. North Korea had already launched several cyber-attacks, including malware and viruses in emails against South Korea, the United States, and Japan. North Korea is copying the Chinese cyber models by recruiting more and more hackers for its army. Despite its old infrastructures, North Korea is a significant cyber actor~~s~~ in the Asian region.

EUROPE

France ~~is~~ creating ~~a~~ national cyber reserve unit

As part of their national cyber defense program, France has decided to create ~~the~~ a specialized national cyber reserve unit. Indeed this new cyber reserve unit will include volunteers of soldiers and analysts, teachers, students undertaking specialized masters in cyber-defense, and students in more general computer training. The national cyber reserve will provide ~~a~~ specific cyber training ~~to be able to~~for managing ~~manage~~ a cyber -crisis. The goal of this unit is to help different agencies in charge of the systems and network security of the country in case of ~~a~~ cyber -warfare or cyber conflict. The concept of cyber reserve is not new, in fact the UK and other countries have already experienced it. Since 2009, France has improved its cyber defense systems and recruited more engineers and cyber specialists to protect its cyber borders. Like the UK, France is trying to be one of the most advanced ~~country's~~ countires in Europe for ~~regarding of~~ cyber defense.

Norway f~~F~~inancial institutions under c~~C~~yber -attack~~s~~ by Anonymous

Norway has been under cyber-attacks conducted by Anonymous Norway, which targeted the financial sector. The hacktivists launched a series of attacks against different Norwegian financial institutions, including the Danske Bank, Norges Bank, Sparebank, and famous insurance companies. However, non-financial corporations have also been targeted, such as Telecom Company and three national airlines. According to the investigation performed by the Evry's security team, the hackers were located outside of Norway and have exploited a vulnerability in the WordPress platform to achieve these attacks. However, they did not ~~steel~~ steal private information from users, the investigation reported; this is typical of normal hacktavist who are not interested in stealing information but rather in creating~~causing~~ publicity for their social or political cause. ~~The~~ Evry's security team added, “The scale is not the largest we have seen, but it is the first time it has hit so many central players in the finance sector in Norway.” Norway has great cyber defense capabilities, and its cyber defense force branch was established in 2012, with about 1,500 people located in 60 different locations. Moreover, Norway has

different computer response teams to handle cyber threats. However, beside its national cyber security policy, Norway is still vulnerable to ~~cyber~~ cyber-attacks and need~~s~~ to improve and strengthen its cyber security to ~~insure~~ ensure ~~a~~ better protection ~~to~~ of its critical infrastructure~~s~~.

NATO approve~~sd~~ ~~the~~ establishment of ~~a~~ military Cyber-Polygon-Base

NATO Defense Forces recently approved the creation of the military Cyber-Polygon-Base in Estonia, which would include the most advanced cyber-laboratory. The major cyber polygon will be deployed in Tallinn, and the preparations have already begun. The polygon will be established on an already existing base, which was constructed in Estonia in 2012, ~~and in which~~where NATO Cyber Forces already conducted the ~~"~~"Cyber Coalition"~~"~~ and ~~"~~"Locked Shields"~~"~~ cyber ~~-~~exercises in 2013. It is likely one of main designations of this joint deployment is the protection from possible Russian aggression scenarios.