UNCLASSIFIED




# Executive Cyber Intelligence Bi-Weekly Report by INSS-CSFI

## August 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

### Chinese cyber espionage campaign against Israel

A major cyber espionage campaign against the Israel defense industry, focusing on the Iron Dome, was published by the blog KrebsonSecurity. According to the publication, the attack took place between the years 2011 and 2012 against three of Israel's major defense contractors – Elisra, Israel Aerospace industries (IAI), and Rafael. An infamous hacker group from China, nicknamed "comment crew" are believed to be behind this attack. The attack began like all other "APT1" attacks, with a well-designed phishing email. In the period of four months, the attackers established a foothold in the network system by installing backdoors, injecting Trojans, and gaining access to sensitive files. At this point, they transferred jumbo files to their own servers. The cyber security firm, cyberESI, tapped into the communication infrastructure set by the hackers to determine that the data stolen was information on the arrow 3 missile system, UAVs, the Iron Dome system, and more. Elisra and Rafael did not respond when asked about the breach, while IAI denied it completely stating the breach was not of a confidential network.

### Anonymous false claims

On 27/07/14, @AnonymousGlobo tweeted they took down a number of Israeli websites, including the Mossad home page and a major bank within Israel. The story of Anonymous taking down the Mossad page was picked up a few days later by the cyber news website, HackRead, with the addition that the Mossad website was still down almost three days later. This claim proved to be false, even though additional cyber news websites began to report this as well as other Anonymous Twitter accounts including @YourAnonNews and @AnonymousPress. The Mossad home page website may or may not have been down for a few minutes; yet, besides the single tweet from @AnonymousGlobo, there had been no additional evidence such as screen shots or confirmations. Anonymous false claims bring up two points: firstly, even with the claim they brought down Mossad, bringing down the Mossad homepage brings little significant effects as it is not connected to the Mossad network system, and secondly, it depicts how Anonymous continues to decline in capabilities of creating long lasting or true cyber-attacks.

## NORTH AMERICA

### Canada accuses China of cyber attacks

At a recent meeting between Canadian Foreign Minister John Baird and Chinese Foreign Minister Wang Yi, Minister Baird accused China of cyber-attacks against Canada's National Research Council (NRC), a research and technology organization with investments in business technology within the government. The details of the attack have not yet been released, but it hinted that personal information of employees and clients of NRC may have been comprised. Minister Baird referred to the cyber hackers as "highly sophisticated Chinese state sponsored actors." The data comprised through this cyber-attack halted with the NRC and the 40 networks to which it is linked. The infiltration was incapable of entering into the Canadian government network. Though Canada did not reveal details of the cyber-attack, the cyber-attack demonstrated similarities to previous hacking campaigns from China; this

is not the first time Canada has been hacked by China. A new and more advanced cyber security program has been ordered for the NRC, though it may take up to year. This is the first instance where Canada has publically accused a country of cyber-attacks. China has denied the allegations and opposed them.

**US House passes two bills on cyber security**

House of Representatives passed two bills regarding cyber security networks. The first bill aimed at limiting cyber-attacks against critical infrastructures through a framework constructed by the Department of Homeland Security. The bill was hailed as the National Cybersecurity and Critical Infrastructure Protection Act. The second focused on enhancing the protection of customer personal information. Currently, both bills are awaiting vote by the Senate.

## RUSSIA

**International operation against leading Russian cyber criminals**

US authorities, in coordination with law enforcement authorities in Spain, the UK, and Canada, conducted a large-scale operation, leading to the arrest of leading Russian cyber criminals. It is assumed the gang leader is 30-year old Russian Vadim Polyakov. He and seven other hackers are suspected of theft of $ 1.6 million from bankcards in Europe.

**Russia offered $111,000 for cracking TOR anonymity**

The Russian government has offered a reward to whomever is able to crack the underground network “The Onion Router” (TOR). TOR is a downloadable system meant to virtually hide users' activities from identification, and many use it for access into the Deep Web, aka ".onion." The Russian Ministry of Internal Affairs explained they want researchers to “study the possibility of obtaining technical information about users and users' equipment on the TOR anonymous network.” Only Russian companies are allowed to be included. This demand is Russia's insurance of its country's national security. Each participant must pay $195,000 to participate and about $5,555 application fees to enter the competition. TOR has been a real frustration for authorities. TOR eliminates a nation’s control on the incoming and outgoing Internet traffic. This announcement from Russia comes after it has been revealed for roughly five months that TOR faced a critical vulnerability to "deanonymize" users. TOR explained that anyone who downloads the most updated system will close the vulnerability; however, the effect of the attack on users had remained unclear. The attackers "modified TOR protocol headers to do traffic confirmation attacks," TOR admitted.

**Azerbaijan becoming part of anti-phishing workshop group**

Azerbaijan Cyber Security Center became a member of the Anti-Phishing Working Group (APWG) and has been accepted to the list of official members of the research team. This entitles them for Research Partnership rights to Research Partners. The APWG was established in 2003 and currently has more than 2000 companies worldwide across industry, government, and law enforcement sectors. Azerbaijan and Georgia officials met to exchange views on the possibilities of cooperation in the field of improving cyber security in the region.

## ARAB COUNTRIES

### Iran to hold cyber security exhibition

Iran is about to organize one of its biggest cyber-security exhibitions. The upcoming event will take place in Teheran from the 27th to the 30th of July, 2015, and is aiming to provide a place for Iranian IT companies to display their new cyber products. This fair will also give the Iranian organizations the opportunity to find the most appropriate cyber security systems to counter cyber threats. Iran has tried to improve both its military and civil critical infrastructure against cyber-attacks. Beside the multiple cyber-attacks the country has experienced since 2010, Iran has developed a great cyber capability. Today the country is known as one of the best countries worldwide for cyber security and is the second in the Middle East after Israel.

### Qatar behind Hamas cyber advancement

Cyber terrorism against Israel has continued since Operation Protective Edge. Though many of the cyber-attacks failed, it has been revealed that almost 70% of all cyber-attacks have come from Qatar. Qatar has emerged during the operation as one of Hamas's biggest supporters and funders. According to Aviad Dadon of Israeli cyber-security firm AdoreGroup, Qatar has taken the initiative to train and advance Hamas's technological capabilities. As Dadon explains: "[The people of Qatar] are taking lessons from the performance of their cyber-equipment and will improve them even further for the next war, which will be even more cyber-oriented than this one."