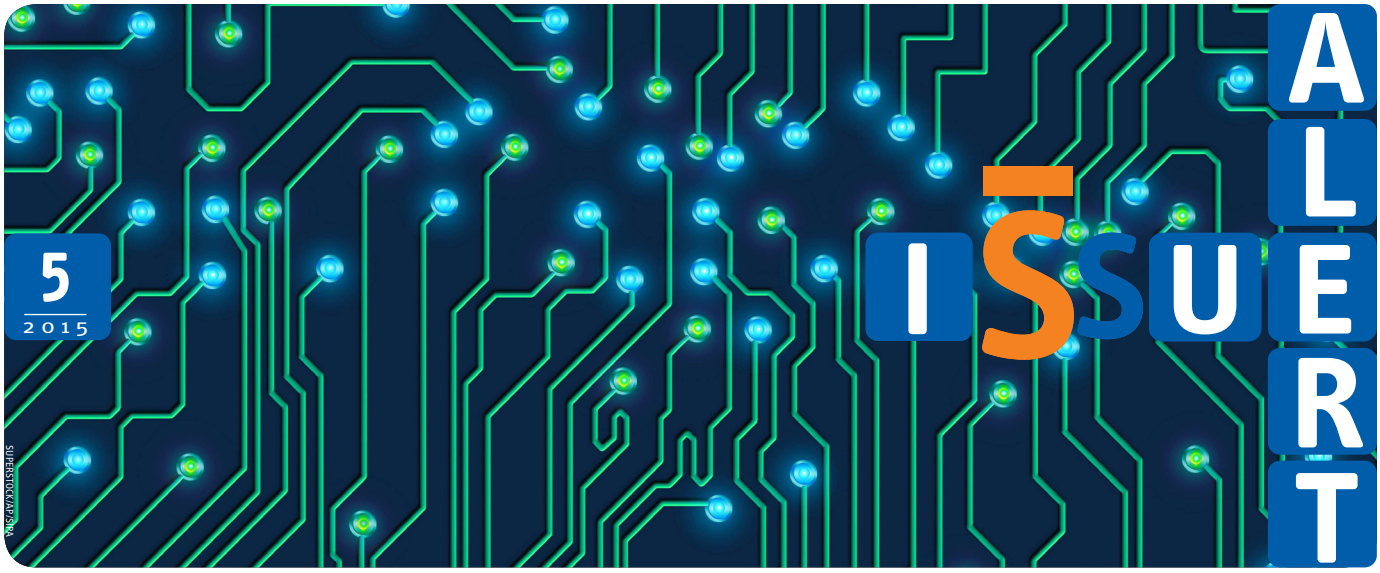

State-sponsored hackers: hybrid armies?

by Patryk Pawlak and Gergana Petkova

Cyber-attacks are rarely disconnected from political realities. CyberBerkut – a pro-Russian group of 'patriot' hackers – has, for example, hacked German government websites in retaliation for the political support offered to Kiev by Berlin. The Syrian Electronic Army – a hacker collective thought to be linked to Syrian President Bassar al-Assad – regularly targets Western media outlets, most recently *Le Monde*.

Due to this blurring of the virtual and physical worlds, governments, which are familiar with stateless actors such as al-Qaeda or the Islamic State of Iraq and the Levant (ISIL), may now have to learn to deal with equally hostile, amorphous and often state-sponsored 'hacktors'.

Using the past but shaping the present

While maritime disputes between China and its neighbours often grab the headlines in the Asia-Pacific, cyber-attacks are comparatively underreported. Each year, for instance, the commemoration of the Sino-Japanese conflict which began on 18 September 1931 (and resulted in Japan's occupation of three provinces in northeast China) witnesses a virtual offensive on Japanese websites.

The '9/18' cyber-attacks in recent years have been fuelled by a host of diplomatic disputes. In 2010, the collision of a Chinese fishing boat with a Japanese coast guard vessel and the subsequent detainment of its Chinese captain and crew caused a flurry of malicious cyber activity. Attacks in later years were triggered by the 80th anniversary of the 1931 Manchuria incident or the ongoing controversy over the Senkaku/Diaoyu islands.

Non-state cyber armies have also been employed in ongoing conflicts. CyberBerkut is but the most recent example: the group not only managed to hack governmental websites in Germany, Ukraine and Poland, but also successfully took down three NATO websites, including that of the Cooperative Cyber Defence Centre of Excellence in Tallinn.

Other Russian political movements, which are organised and partially sponsored by the state, also have an important role in non-state cyber offensive capabilities. For instance, a group called 'Nashi' claimed responsibility for the Distributed-Denial-of-Service attack in Estonia in 2007. The group is also active domestically, targeting the Russian opposition and those critical of the government, including newspapers such as *Kommersant*.

Smaller and militarily less advanced countries appear to readily embrace the actions of such 'patriotic' hackers as they benefit from the tactical asymmetry – a sort of virtual guerrilla warfare – that the cyberspace offers. The Syrian Electronic Army, active since the outbreak of protests in Syria

in 2011, claims to be driven by patriotism and denies any official affiliation with the government. The group is behind some of the more audacious cyber-attacks, including the defacement and hacking of numerous media websites and Twitter accounts (e.g. the BBC, *The Guardian*, *The New York Times*, Human Rights Watch, and *Forbes*), opposition Facebook pages, chat messengers like Skype and Viber, as well as foreign government institutions (e.g. Saudi Arabia's Ministry of Defence).

Examples of malware and state-linked cyber-attacks

Flame: Malware described as 'the most sophisticated cyber weapon yet unleashed'. Detected in the Middle East, it shares many characteristics with Duqu and Stuxnet. Flame begins by sniffing the network traffic, taking screenshots, recording audio conversations, and intercepting keyboard presses.

Red October: Malware used for a cyber-espionage campaign that has affected hundreds of bodies around the world – including diplomatic and government agencies, research institutions, energy and nuclear groups, and trade and aerospace organisations.

MiniDuke: Malware designed to steal data from government agencies and research institutions. Kaspersky Labs uncovered 59 high-profile victim organisations in 23 countries, including Belgium, the Czech Republic, Hungary, Ireland, Portugal, Romania, Ukraine, and the US.

GhostNet: Malware allegedly originating in China which infiltrated targets in about 103 countries, including the systems of NATO SHAPE headquarters, various embassies and foreign ministries, and the office of the Dalai Lama.

Moonlight Maze – Suspected state-sponsored attacks by Russian hackers targeting the Pentagon, the US Department of Energy, NASA and several universities and research labs.

Titan Rain – Suspected state-sponsored attacks by Chinese hackers targeting the computer networks of US defence contractors in search of military secrets. The networks of the British and German governments appear to have been targeted at the same time.

Looking into the future

In addition to governmental or political targets, state-linked hackers have also damaged private businesses. In 2014, the US-based security company Crowdstrike blamed a Chinese PLA-associated group 'Putter Panda' for a series of cyber-espionage actions directed at high-profile aerospace, satellite and communications targets. More recently, another group called 'Guardians of Peace' – supposedly linked to North Korea – claimed responsibility for an attack on Sony Entertainment Pictures which resulted in the loss of personal information of employees and their families and the exposure of executive-level salaries and company email exchanges.

Available data suggest that cyber-espionage by state-affiliated groups is on the rise. The 2014 Data Breach Investigations Report by Verizon, a US telecommunications company, shows that 87% of all such incidents in 2013 (511) were performed by state-linked groups originating from either East Asia (49%) or eastern Europe (21%).

With state and non-state actors ever more interested in developing both offensive and defensive cyber capabilities, designing the rules of the game will be complicated. Authoritarian regimes enjoy significant freedom to set and adapt rules as they please. Their opponents have, alas, more limited options. In democratic states, governments are bound by the rule of law and operate under strict public scrutiny. Legal cooperation among like-minded countries is moving forward, but at a very slow pace.

Little can be done if certain actors choose not to play by the rules. The US indictment of five Chinese military officers for cyber-espionage in 2014 was, for example, practically ignored by Beijing. And the use of sanctions – as was the case against North Korea following the attacks on Sony – may just aggravate the delicate situation on the peninsula further.

Accordingly, a preventive cyber-attack on – or quick retaliation against – the computer networks of other countries suspected of providing support to hackers may appear the only response capable of deterring future incidents.Such actions, however, may undermine the international system in the long run – and further muddy the already difficult international debate surrounding cyber norms.

Patryk Pawlak is a Senior Analyst and Gergana Petkova is a Junior Analyst at the EUISS.

 | QN-AL-15-005-2A-N | ISBN 978-92-9198-300-1 | ISSN 2315-1129 | DOI 10.2815/341983