CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 05 – May 2016

EXECUTIVE SUMMARY

Keywords: *Active Cyber Defence, Cyber Intelligence, Cyber Warfare, G7, Iran, Japan, Strategy, Supreme Council of Cyberspace, United Nations, United States, U.S. Naval Academy.*

At the end of May, the leaders of the G7 met in Ise-Shima, Japan, to discuss major global political and economic challenges. Cyber security has played a leading role as one of the numerous subjects addressed, and experts in the field will surely appreciate the document issued entitled "G7 *Principles and Actions on Cyber*".

The G7 document focuses not only on a just and always desirable reaffirmation of the principles promoting protection of human rights, privacy and personal data, as well as cooperation and information sharing to tackle terrorism and cyber crime. Interestingly enough, the G7 openly recognises the possibility that ITC attacks may in some circumstances amount to the use of force or armed attacks under customary international law and the UN Charter. Hence, it follows that States may exercise their right to engage in individual or collective self-defence, in compliance with Art. 51 of the UN Charter.

Despite the progress made up to now, the creation of an international framework of globally shared and recognised regulations for the use of offensive capabilities in and through cyberspace is now one of the main goals for all governments. This, to prevent the so-called "militarization of cyber space" from getting particularly blurred boundaries, in the absence of clear State behaviour regulations.

Instead, from each State's perspective, the Japanese government has publicly announced the creation of an agency tasked with protecting its critical infrastructures from cyber attacks.

The *Industrial Cybersecurity Promotion Agency* – this the prospective name of the agency – will be a public-private body, starting working in 2017 thanks to huge investments from private entities.

The agency shall be positioned as an extra-governmental body affiliated with the Ministry of Economy, Trade and Industry, and shall have two main functions: first to increase specific technical and technological know-how in cyber security, secondly to coordinate and conduct researches to develop countermeasures to handle cyber attacks against Japanese national critical infrastructures.

During the month of May, also the Tehran's government has made headlines. Speaking through its *Supreme Council of Cyberspace*, in fact, it has officially requested foreign providers of social media and instant messaging services to transfer into the Iranian territory the data centers in charge of processing and filing Iranian citizens' data.

This latest decision taken by the government shows Iran is afraid that technology and the Internet might let Western concepts, ideals and lifestyles seep into the Country's social fabric, clashing with the present political leaderships' interests or undermining these latters' stability.

The above clearly shows Teheran government is having a defensive approach so as to reach two main goals. The first one – as also detailed in February 2016 *"Cyber Strategy & Policy Brief"* – is to protect the Country's critical infrastructures from cyber attacks mainly coming from Saudi Arabia and the pro-Ryad Gulf Countries, as well as from the USA and Israel. The second one is to protect the government leadership containing propaganda and information activities spread in cyberspace by opposition parties and social and political dissent groups.

Finally, at the end of May the U.S. Naval Academy graduated its first 27 "*Cyber Operations*" Midshipmen.

It is the first time ever for a U.S. military school to offer officers a complete course of studies dedicated to military operations in and through cyber space.

Educating and training future officers of the Armed Forces to military operations in and through the cyber space with specific courses of studies seems an ever more real and tangible need. The current scenario, indeed, shows that even in the short period technologies and the Internet in military activities will play a more and more considerable role, particularly when facilitating kinetic attacks.

An alphabetic list follows of the main cyber security related news and events of the last months about strategy and policies.

FOCUS ON "*G7 PRINCIPLES AND ACTIONS ON CYBER*"

At the end of May, the leaders of the G7 met in Ise-Shima, Japan, to discuss major global political and economic challenges. Cyber security has played a leading role as one of the numerous subjects addressed, and experts in the field will surely appreciate the document issued entitled "*G7 Principles and Actions on Cyber*".

Furthermore, it needs to be stressed that it is the first time ever that the G7 leaders decide to set out a specific document totally dedicated to principles and actions to be taken in the field of cyber security.

Such a shared interest hereto at such high institutional levels traces back to five years ago, at the e-G8 Forum, convened in 2011 by the French President Sarkozy prior to the 37th G8 summit.

Nevertheless, it is not a case that this document has been drafted and issued at a summit hosted by Japan, long since prioritising cyber security in its political and strategic agenda.

The G7 document focuses on subjects that are perfectly in line with the strategic approach followed by the main Western countries worldwide, as well as with European cyber strategy.

However, it deals not only with a just and always desirable reaffirmation of the principles promoting protection of human rights, privacy and personal data, as well as cooperation and information sharing to tackle terrorism and cyber crime. Interestingly enough, the G7 openly recognises the possibility that ITC attacks may in some circumstances amount to the use of force or armed attacks under customary international law and the UN Charter.

Hence, it follows that States may exercise their right to engage in individual or collective self-defence, in compliance with Art. 51 of the UN Charter.

Such a trend shows – as already stressed more than once (see January, March and April 2016 "*Cyber Strategy & Policy Brief*") – how the strategic approach of the main global powers is rapidly shifting from a simple active defence (*Active Cyber-Defence*) to a real development of offensive capabilities for cyberspace. All the above in the absence of clear international strategies hereof and especially in the absence of an international framework of globally shared and recognised regulations for the use of offensive capabilities in and through cyberspace.

In this regard, anyway, it needs to be highlighted that back in 2013, following the meeting of the *UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, it was agreed that international law in force also applies in the "cyber domain", as well as traditional concepts of State sovereignty.

A more detailed definition of such principles followed in 2015. In fact, the latest report from the *UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* expressly maintains, *inter alia*, that:

a. States have jurisdiction over the ICT infrastructure located within their territory;
b. In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms;
c. […]
d. The Group notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction;
e. States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts;
f. States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated.

Despite the progress made up to now, the creation of an international framework of globally shared and recognised regulations for the use of offensive capabilities in and through cyberspace is now one of the main goals for all governments. This, to prevent the so-called "militarization of cyber space" from getting particularly blurred boundaries, in the absence of clear State behaviour regulations.

IRAN

At the end of May the government of Teheran, speaking through its *Supreme Council of Cyberspace*, officially requested foreign providers of social media and instant messaging services to transfer into the Iranian territory the data centers in charge of processing and filing Iranian citizens' data. Abolhassan Firouzabadi, secretary of Iran's *Supreme Council*, also announced that such a data transfer shall take place within a year. Failure to comply shall result in exclusion of such services from the territory.

Bearing in mind that approximately half the Iranian population (39 Million people) own smart phones, the market of social media and instant messaging services has almost 14 Million users. According to an official survey carried out by the Ministry of Youth Affairs and Sports back in 2013, 69,3% of youngsters habitually bypass filtering imposed by the government to use these services. Hence, although applications such as Telegram (counting 20 Million users) and Instagram are the most used Western services in Iran, use of social networks such as Facebook and Twitter is, instead, blocked by institutional filters.

President Rouhani's and the Iranian Government's approach is not new at all. Several forms – even more capillary and indiscriminate – of control and repression towards such services can be traced back to 2009, during Ahmadinejad's presidency.

Moreover, it needs to be stressed that the *Supreme Council of Cyberspace* has incorporated a special committee to monitor social media contents, made up of Intelligence, Interior and Culture Ministries and Iranian Cyber Police representatives.

The above clearly shows Teheran government is having a defensive approach so as to reach two main goals. The first one – as also detailed in February 2016 *"Cyber Strategy & Policy Brief"* – is to protect the Country's critical infrastructures from cyber attacks mainly coming from Saudi Arabia and the pro-Ryad Gulf Countries, as well as from the USA and Israel. The second one is to protect the government leadership containing propaganda and information activities spread in cyberspace by opposition parties and social and political dissent groups.

Finally, this latest decision taken by the government shows Iran is afraid that technology and the Internet might let Western concepts, ideals and lifestyles seep into the Country's social fabric, clashing with the present political leaderships' interests or undermining these latters' stability.

JAPAN

During the month of May, the Japanese government has publicly announced the creation of an agency tasked with protecting its critical infrastructures from cyber attacks.

The *Industrial Cybersecurity Promotion Agency* – this the prospective name of the agency – will be a public-private body, starting working in 2017 thanks to huge investments from private entities.

The agency shall be positioned as an extra-governmental body affiliated with the Ministry of Economy, Trade and Industry, and shall have two main functions: first to increase specific technical and technological know-how in cyber security, secondly to coordinate and conduct researches to develop countermeasures to handle cyber attacks against Japanese national critical infrastructures.

Nevertheless, Japan commitment to critical infrastructures security shouldn't surprise. Several Japanese governments have in fact prioritised cyber security in the country's political and strategic agenda: since 2005 through the first "*Action Plan on Information Security Measures for Critical Infrastructures*" up to today's third edition of "*Basic Policy of Critical Information Infrastructure Protection*".

It seems obvious, then, that protection of critical infrastructures from cyber attacks is one of the main strategic pillars Japan cyber strategy is grounded on.

The strategic document, updated in September 2015, points out such a need, and indicates the sectors to be considered as critical. Indeed, it also outlines three different operative actions making protection of critical infrastructures as effective and efficient as possible.

These include conducting a continuous revision of methods and tools used to protect critical infrastructures, implementing – as far as possible – the same methods and tools in private companies, sharing information on threats as an essential element, and creating a governmental support that can make ITC systems security even more reliable. With regard to the above, Prime Minister Shinzo Abe's goal is to focus the government attention on the protection of Japanese citizens and systems, providing them with basic services and main economic activities.

Conversely, a certain grey area exists on the reason why Japanese government has decided to position the *Industrial Cybersecurity Promotion Agency* within the Ministry of Economy, Trade and Industry.

Considering that protection of critical infrastructure is maybe the main factor to guarantee security of a country and its citizens and economic wellbeing of a State, such a structure should have been naturally and ideally positioned within the Japanese *National Information Security Center*.

Hence, although *Industrial Cybersecurity Promotion Agency*'s goal is to increase specific technical and technological know-how in cyber security, as well as to coordinate and conduct researches to develop countermeasures to handle cyber attacks against Japanese national critical infrastructures, it is the *National Information Security Center*'s duty to analyse and counter cyber attacks against Japanese governmental networks.

The inclusion of the *Industrial Cybersecurity Promotion Agency* within the *National Information Security Center* might lead to the creation of a right synergy between operational needs and modes of development and research, currently fuelling growth in this field.

To conclude, this structure would replicate the tendency followed by the main economic powers for a long time now to position cyber security related structures and competencies within single and shortest management lines possible (see January, March and April 2016 "*Cyber Strategy & Policy Brief*").

UNITED STATES

At the end of May the U.S. Naval Academy graduated its first 27 "*Cyber Operations*" Midshipmen.

It is the first time ever for a U.S. military school to offer officers a complete course of studies dedicated to military operations in and through cyber space.

In spring 2013, in fact, the U.S. Naval Academy first announced the intention to offer a three-year major completely focused on this sector, to go along with classic technical and IT majors.

However, the major *in "Cyber Operations*" does not simply provide education and training on the purely technical and technological aspects of IT security, cryptography, programming and forensics. It also offers the future U.S. Navy leaders knowledge and expertise in areas such as policy, law, and even social engineering.

The absolutely cutting-edge approach – for Western countries – of the U.S. Naval Academy cannot but represent an example to be followed by any country, especially in the military field.

Educating and training future officers of the Armed Forces to military operations in and through the cyber space with specific courses of studies seems an ever more real and tangible need. The current scenario, indeed, shows that even in the short period technologies and the Internet in military activities will play a more and more considerable role, particularly when facilitating kinetic attacks.

Even more so, from a global point of view, both in light of the content of the above-mentioned "*G7 Principles and Actions on Cyber*" document, and due to the forthcoming and crucial decision of the Ministers of Defence of NATO countries to officially declare cyber space a warfare domain, as well as land, air, sea and space (this subject will be addressed in next volume of the "*Cyber Strategy & Policy Brief*").

ABOUT THE AUTHOR

Stefano Mele is an attorney specialized in ICT Law, Privacy, Information Security and Intelligence and works as '*of Counsel*' at Carnelutti Law Firm, Milan. He holds a PhD from the University of Foggia and cooperates with the Department of Legal Informatics at the Faculty of Law of the University of Milan. Stefano is also the Founding Member and Partner of the Moire Consulting Group and he is also the President of the "*Cyber Security Working Group*" of the American Chamber of Commerce in Italy (AMCHAM). He is Director of the "*InfoWarfare and Emerging Technologies*" Observatory of the Italian Institute of Strategic Studies 'Niccolò Machiavelli' and member of the International Institute for Strategic Studies (IISS). Stefano is also a lecturer for several universities and military research institutions of the NATO and the Italian Ministry of Defence and has published a number of scientific works and articles about cyber security, cyber intelligence, cyber terrorism and cyber warfare.
In 2014, his name appeared in the list of NATO *Key Opinion Leaders for Cyberspace Security*.
In 2014, the business magazine Forbes listed Stefano as one of the world's best *20 Cyber Policy Experts* to follow online.

For more information: www.stefanomele.it

SEE ALSO THE PREVIOUS VOLUMES

Cyber Strategy & Policy Brief (Volume 1 – January 2016)

Keywords: *Active Cyber Defence, China, Cyber Warfare, Deterrence, GCHQ, Israel, NSA, People's Liberation Army, United Kingdom, Russia, United States, Strategy, U.S. Cyber Command, Ukraine.*

Cyber Strategy & Policy Brief (Volume 2 – February 2016)

Keywords: *Cyber Intelligence, Cyber Warfare, Iran, Islamic State, Italy, North Korea, Saudi Arabia, Strategy, Terrorism, United States, White House*.

Cyber Strategy & Policy Brief (Volume 3 – March 2016)

Keywords: *Cyber Command, Cyber Intelligence, Cyber Warfare, Denmark, Deterrence, GCHQ, Iran, Marine Corps, Strategy, Syrian Electronic Army, United Kingdom, United States*.

Cyber Strategy & Policy Brief (Volume 4 – April 2016)

Keywords: *Australia, China, Cyber Intelligence, Cyber Warfare, Germany, Information Dominance, Russia, Strategy, United States, U.S. Air Force*.