CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 06 – June 2016

EXECUTIVE SUMMARY

Keywords: *Cyber Command, Cyber Intelligence, Cyber Warfare, Israel, Israel Defense Forces, Italian Joint Command for Cyberspace Operations, Italian Joint C4 Command, Italy, NATO, Strategy, Ukraine, Ukraine National Cybersecurity Coordination Centre.*

Last June 14th, the Ministers of Defence of NATO countries recognized cyberspace as the fifth domain of warfare, after land, sea, air, and space. A formal official statement then followed at the 27th NATO summit of the heads of state and government held in Warsaw at the beginning of July.

As a consequence of this most important and by now expected recognition – affecting all the NATO countries – member states shall at soonest discuss earnestly and in detail the elements such a statement should be grounded in.

This, especially in light of the extension to cyberspace of the scope of collective defence provision, dating back to September 2014, according to which NATO countries commit to provide mutual assistance also in case of aggression carried out by means of cyber attacks.

Nevertheless, although in this field NATO mainly aims and will aim to protect its IT systems and help member states develop the most appropriate cyber defence capabilities, after recognizing cyberspace as a domain of warfare, NATO policies shall inevitably evolve – also in the short period – to include cyberspace in collective defence scope.

To this end, as already happens with conventional weapons, every single NATO state and NATO itself shall develop at soonest offensive capabilities for cyberspace, possibly by creating a specific *Cyber Command*. Obviously, they could use such offensive capabilities exclusively in response to (cyber and conventional) attacks carried out against NATO or an allied country.

Furthermore, during the month of June, both the Italian and Israeli governments publicly announced their intention to establish a *Cyber Command*.

The Italian *Joint Command for Cyberspace Operations* (*Comando Interforze per le Operazioni Cibernetiche – CIOC*), whose first unit might already be operational within a year, will have two functions. On the one hand, it will be responsible for the protection of Italian national security, enhancing capabilities to protect from cyber attacks. On the other, it shall develop the Computer Network Operations (CNO) planning and management capabilities in support to military operations both in Italy and abroad.

The Israeli *Cyber Command*, instead, positioned within the *Israel Defense Forces*, shall be operational within two years and shall be responsible for offensive and defensive military operations in and through the cyberspace, centralizing the activities carried out respectively by *Military Intelligence Directorate Unit 8200* and *C4I Telecommunications Directorate*.

It will be interesting to see in the future where exactly the prospective *Cyber Command* shall be positioned within the complex Israeli governmental organization for cyber security and the synergies built with the other, already existing governmental bodies and agencies.
Indeed, agencies such as the *National Cyber Bureau*, responsible for advising and making recommendations on national cyber policy to the prime Minister, and the *National Cyber Security Authority*, responsible for the protection of critical infrastructures and Israeli national CERT, are extremely active and well-organized also in this field, as well as intelligence agencies such as *Shin Bet* and *Mossad*.

Finally, also Ukraine took a big step in the field of cyber security. At the beginning of June, in fact, President Petro Porošenko signed the decree to establish the first Ukrainian *National Cyber Security Coordination Centre*.

The establishment of this *Centre* is in line with the recent release of the first Ukrainian cyber strategy, since March 2016 tasking the *National Security and Defense Council* with the coordination of all governmental agencies involved in cyber security related activities.

The *National Cyber Security Coordination Centre* shall, *inter alia*, coordinate activities in the field of national security and Defence of the governmental bodies responsible for implementing cyber strategy, increase the effectiveness of public administration in the development and application of national cyber security policies, and help regulations to enter in force for the protection of national information resources, classified information, and national critical infrastructures from cyber threats.

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

ISRAEL

At the end of June, *Israel Defense Forces* (IDF) publicly announced its intention to make its *Cyber Command* operational within two years.

The *Command* – whose seat is still unknown – shall be responsible for offensive and defensive military operations in and through the cyberspace, centralizing the activities carried out respectively by *Military Intelligence Directorate Unit 8200* and *C4I Telecommunications Directorate*.

It is indeed clear that the Israeli government is following in the path of the main international players (see also in this document the recent decisions of the Italian government).

The trend is in fact to centralize both defensive and offensive capabilities and competences in the field of cyber intelligence and cyber warfare under a single chain of command that is as short as possible. This, not only to optimize the constantly growing economic investments, but especially to enhance operational efficiency and effectiveness of the organizations active in and through the cyberspace, making them more streamlined and responsive (for details on the U.S. and China, see in particular January 2016 "*Cyber Strategy & Policy Brief*").

Cyber attacks are in fact increasingly seen as an integral part not only of policies to protect national security, but also of policies aimed to reach state goals and interests.

Furthermore, it will be interesting to see in the future where exactly the prospective *Cyber Command* shall be positioned within the complex Israeli governmental organization for cyber security and the synergies built with the other, already existing governmental bodies and agencies.
Indeed, agencies such as the *National Cyber Bureau*, responsible for advising and making recommendations on national cyber policy to the prime Minister, and the *National Cyber Security Authority*, responsible for the protection of critical infrastructures and Israeli national CERT, are extremely active and well-organized also in this field, as well as intelligence agencies such as *Shin Bet* and *Mossad*.

In light of this, one of the main strategic pillars for the prospective *Cyber Command* should be reaching maximum levels of cooperation and information sharing.

Together with many others, it is a crucial aspect that can hopefully find a well-arranged and coherent place in a specific cyber strategy that, at least for the time being, Israel is still lacking.

ITALY

The "*White Book for International Security and Defence*", drafted by the Italian Ministry of Defence and approved in April 2015, recognizes cyber defence and military operations in cyberspace as one of its strategic priorities and one of the main investment programs for the period 2016-2018.

To this end, the Italian Defence has planned to create, *inter alia*, a *Joint Command for Cyberspace Operations* (*Comando Interforze per le Operazioni Cibernetiche – CIOC*).

The *Command* will have two functions. On the one hand, it will be responsible for the protection of Italian national security, enhancing capabilities to protect from cyber attacks. On the other, it shall develop the Computer Network Operations (CNO) planning and management capabilities in support to military operations both in Italy and abroad.

Although only little information is presently available, recent statements released by officers of the Italian Armed Forces showed that, despite still being at an initial stage, the first *Joint Command for Cyberspace Operations* operative unit might already be operational within a year. Nonetheless, at least for the moment, the focus seems to be especially on the organization of the *Command*, technologies needed to operate it, staff required and their training.

As per its organizational structure, instead, the Italian *Joint Command for Cyberspace Operations* shall most likely respond to the Chief of Defence Staff (*Capo di Stato Maggiore della Difesa – CaSMD*) – in his capacity as technical and military head of the Italian Defence – and especially to his Vice Commander for Operations (*Vice Comandante per le Operazioni* – VCOM-OPS), responsible for operational planning and deployment of forces in military operations, cyber operations included.

Furthermore, as a *Defence Joint C4 Command* already exists within the Italian Defence, with the purpose of managing joint activities aimed at ensuring the efficiency of command, control, telecommunications and ITC, it seems likely that the prospective *Joint Command for Cyberspace Operations* shall be positioned within the *Defence Joint C4 Command*, completely taking over the IT part and therefore also the Italian *Defence CERT Technical Center*.

Finally, despite not being clearly defined in the Ministry of Defence multi-year economic planning document, funding for cyber defence in Italy is included and distributed into the more sizeable funding for "*Joint C4I Systems*".
Notwithstanding, since such document defines the enhancement of cyber defence capabilities as one of the most significant funding programs for the Italian Defence, it is likely that the

highest percentage of the about €.22.4 million allocated for "*Joint C4I Systems*" in the period 2016-2018 shall be assigned to this field.

All the above proves Italy is following the approach of other countries also with regard to the creation of a specific *Cyber Command*.
Although as of now it is quite difficult to understand how many and what countries have created a specific command for military operations in and through the cyberspace, around 60 countries have already developed cyber defence units. The figure goes up to 100 countries, including those about to develop them.

The activities of the *Defence Joint C4 Command* have long helped Italy face cyberspace as a domain to protect from and to protect the Italian national security.
Moving toward the prospective Italian *Joint Command for Cyberspace Operations*, therefore, cannot but be welcomed positively, especially looking at how the main international players have developed their defensive capabilities in and through the cyberspace in the last few months (for details, see in particular January, March, April, and May 2016 "*Cyber Strategy & Policy Brief*").

NATO – FOCUS ON CYBERSPACE AS A DOMAIN OF WARFARE

Last June 14th, the Ministers of Defence of NATO countries recognized cyberspace as the fifth domain of warfare, after land, sea, air, and space. A formal official statement then followed at the 27th NATO summit of the heads of state and government held in Warsaw at the beginning of July.

As a consequence of this most important and by now expected recognition – affecting all the NATO countries – member states shall at soonest discuss earnestly and in detail the elements such a statement should be grounded in.

This, especially in light of the extension to cyberspace of the scope of collective defence provision, dating back to September 2014, according to which NATO countries commit to provide mutual assistance also in case of aggression carried out by means of cyber attacks.

Nevertheless, although in this field NATO mainly aims and will aim to protect its IT systems and help member states develop the most appropriate cyber defence capabilities, after recognizing cyberspace as a domain of warfare, NATO policies shall inevitably evolve – also in the short period – to include cyberspace in collective defence scope.

To this end, as already happens with conventional weapons, every single NATO state and NATO itself shall develop at soonest offensive capabilities for cyberspace, possibly by creating a specific *Cyber Command*. Obviously, they could use such offensive capabilities exclusively in response to (cyber and conventional) attacks carried out against NATO or an allied country.

NATO shall therefore explain as clearly and effectively as possible how such offensive military capabilities for cyberspace can integrate in its defence and deterrence from attacks strategy.

Presently, the most viable solution is to develop a doctrine and procedures that can be useful to turn cyber attacks into military operational capabilities and give NATO the broadest spectrum of options to deter adversaries' cyber attacks.

Several critical aspects are to be overcome while implementing such a process. Firstly, a clear-cut distinction has to be made between activities NATO can carry out in the field of cyber defence in peacetime and cyber attacks to be possibly conducted as part of real military operations or in execution of the collective defence clause.

It might also be critical not only to decide upon the threshold beyond which a cyber attack can equal a conventional attack, but also upon the proportionality level of cyber reactions compared to the damage suffered from as a consequence of the attack undergone.

Despite all these critical aspects, however, nowadays the creation of an international framework of globally shared regulations for the use of offensive capabilities in and through cyberspace must be urgently recognized as one of the main goals for all governments and international organizations, as also outlined in May 2016 "*Cyber Strategy & Policy Brief*". This, to prevent the so-called "militarization of cyber space" from getting particularly blurred boundaries, in the absence of clear State behavior regulations.

UKRAINE

At the beginning of June, President Petro Porošenko signed the decree to establish the first Ukrainian *National Cyber Security Coordination Centre*.

The establishment of this *Centre* is in line with the recent release of the first Ukrainian cyber strategy, since March 2016 tasking the *National Security and Defense Council* with the coordination of all governmental agencies involved in cyber security related activities.

It is not a case, in fact, that the *National Cyber Security Coordination Centre* will be positioned within the *National Security and Defense Council*, headed by its Secretary, Oleksandr

Turchynov. In addition, members of the *Centre* will be the high representatives of the Ministry of Defense, the Chief of the General Staff of the Armed Forces, the Chairmen of the Ukrainian intelligence services (*Sluzhba Bezpeky Ukrayiny* and *Sluzhba Zovnishnoi Rozvidky Ukrainy*), the National Police, National Bank of Ukraine and members of governmental agencies active in the field of cyber security.

The *National Cyber Security Coordination Centre* shall, *inter alia*, coordinate activities in the field of national security and Defence of the governmental bodies responsible for implementing cyber strategy, increase the effectiveness of public administration in the development and application of national cyber security policies, and help regulations to enter in force for the protection of national information resources, classified information, and national critical infrastructures from cyber threats.

The implementation of a cyber strategy first and then the creation of the *National Cyber Security Coordination Centre* certainly represent a big step forward for President Porošenko government in the field of cyber security. An Ukrainian electrical plant has, in fact, recently undergone the first – publicly known – cyber attack causing tangible consequences on Ukrainian population.

On December 23rd, 2015, indeed, the energy companies *PrykarpattiaOblEnergo* and *KyivOblEnergo*, providing energy to the Western region of Ukraine, claimed to have undergone a cyber attack to the management systems of many of their energy grids, causing a widespread and prolonged power outage in a vast area of the region and leaving over 225,000 citizens without electricity (for further details, see January 2016 "*Cyber Strategy & Policy Brief*").

As a consequence of such recent events and also in light of the evolving strategic approach of other countries to this field, it is not surprising that also Ukrainian cyber strategy provides for the creation of a military unit exclusively dealing with "*Active Cyber Defence*". In fact, although Ukrainian cyber strategy is overall highly defensive, Porošenko government's military approach against future cyber attacks clearly looks much more reactive. As also outlined in the previous editions of "*Cyber Strategy & Policy Brief*" (see in particular January, March, April, and May 2016 "*Cyber Strategy & Policy Brief*"), in so doing, Ukraine is chasing the approach of the main international players, more and more committed in developing offensive capabilities to conduct military operations in and through the cyber space.

Finally, while comments on the implementation level of Ukrainian cyber strategy through the activities of the *National Cyber Security Coordination Centre* can be left for the future, it needs to be highlighted that Porošenko government's strategic approach is lacking a key – but highly underrated – element that is public-private cooperation.

Actually, public-private cooperation has been included in the *Action Plan* for implementing Ukrainian strategy, approved by the Ukrainian Council of Ministers at the end of June. Nonetheless, the important and central role it plays in cyber security needs to be further stressed in any case.

The features of cyberspace, in fact, make large-scale cooperation absolutely necessary and fundamental, in this field more than in others. This is due especially to the fact that not all of those involved in such "domain" can have – on their own – a total overview of cyber threats and all the information needed to face and tackle them.

The government must therefore necessarily establish close relationships with private stakeholders, not seldom owning the vast majority of critical infrastructures, as it is often not in a position to independently gain the so-called "relevant information" on operative techniques, tools and technologies used, at times not even on the strategies adopted by the players active in and through the cyberspace.

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 01 – 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 02 – 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 03 – 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 04 – April 2016)

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

Cyber Strategy & Policy Brief (Volume 05 – May 2016)

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