WHY A CYBER STRATEGY & POLICY BRIEF?

The high level of pervasiveness of technologies and the Internet in every field of today’s social fabric has completely changed every aspect of our society, service delivery and management, access to information – in both its quality and quantity – as well as the relationship between the aforementioned elements and the citizens, what’s more, in a rather limited stretch of time. As if that wasn’t enough to highlight their paramount importance in the so-called “information society”, technologies and the Internet are at the root of those complex systems that ensure the correct functioning of a state’s strategic and critical sectors, namely energy, communication, transports, finance and so on. Hence, they function as one of the pivots around which each country’s economic and social well-being revolves as well as its support and the starting point for its growth.

Moreover, the analysis of the current scenario and the most relevant national cyber security strategies define the most evident features of the threats. These are mainly due to the low level of perception and awareness of these issues, to a supranational regulatory vacuum, poor domestic and international cooperation, and it is also due to the low level of ability of national critical systems to reach adequate standards of computer security and resilience.

Guaranteeing a strategic approach to the security of this sector and planning its growth, assessing short, medium and long term risks as well as producing forecasts on its evolution are therefore an essential and priority task in each good government’s political agenda. This is true especially nowadays, when the protection of the cyberspace represents a top priority challenge.

The Cyber Strategy & Policy Brief aims at raising the reader’s awareness on these issues, by monthly analysing the main international events, in order to highlight the trends of cyber threats and the lessons learned that might be useful to protect national security.
EXECUTIVE SUMMARY

Between the end of 2015 and the beginning of 2016 several significant cyber security related events have taken place, that analysts cannot leave behind, including the release of some crucial strategic documents and cyber attacks launched to critical national infrastructures. This trend shows cyber security issues are still growing and a huge number of attacks are undermining the national and economic security of the main international players.

Furthermore, the strategic approach of the main international players is quickly shifting from a mainly active cyber defence to the development of offensive cyber capabilities.

All the above, with no clear and consolidated strategies from international organisations and without an internationally recognised framework of regulations to govern the use of offensive cyber capabilities.

Moreover, speaking about the organizational structure, the trend for some of the main global leaders (USA and China ahead) is to centralize under a single and faster chain of command defensive and offensive capabilities and expertise in the fields of cyber intelligence and cyber warfare. The aim of such a reorganization seems to be rationalizing greater and greater economic investments and increasing the effectiveness and efficiency of entities/agencies active in and operating through cyber space, to make them simpler and more responsive.

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

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.
CHINA

Last December 31st, the Chinese Central Military Commission publicly announced to have recently conducted a reorganization of the People’s Liberation Army – Chinese army, leading to the establishment of three new branches: Army Leading Organ, Rocket Force and Strategic Support Force.

Of the three, the Strategic Support Force stands out with regard to cyber security. Official sources have confirmed that it might, in turn, have three branches: the first one dealing with intelligence and military operations in cyber space (both defensive and offensive); the second one dealing with space military operations (including surveillance and satellite), and the third one in charge of defensive and offensive Electronic Warfare (EW) and Intelligence (ELINT). Hence, the Strategic Support Force seems to be taking on soon the duties of People’s Liberation Army Third and Fourth Department. By doing so, two of what Chinese strategic documents call “critical domains” – space and cyber space (the third one being the nuclear) – will be under the same chain of command.

Such reorganization is no surprise, actually. Indeed, Chinese strategy has always endorsed an “Integrated Network and Electronic Warfare” approach, combining Cyber Warfare and Electronic Warfare, on the one hand, while moving the concept of Information Warfare toward that of “Information Confrontation”, on the other. Strategically speaking, the only next step to be taken was to gather all Information Warfare elements (both military and intelligence; both defensive and offensive; both electronic and cyber) under the same chain of command, now nearer than in the past to the influence of the Central Intelligence Commission.

ISRAEL

It’s been a long time since the Israeli government has focused on cyber security (both military and intelligence) as a means to protect its national strategic interests and as a driving force for economic development. It took only three years for Israel to reach worldwide the top of the list in this field, thanks to the new Be’er Sheva “CyberPark”, totally addressed to cyber security issues. Recent official surveys show that Israel is presently home to over 300 companies active in the cyber security field, with an export (facilities and technology) turnover of 6 billion $, representing the 20% of private investments in this field worldwide. Such figures and their continual increase, in January led Prime Minister Netanyahu to promote Be’er Sheva “CyberPark” not only as the centre of Israel’s cyber security, but also as a global point of reference in the cyber security field. This is also due to the fact that European countries have
overlooked this kind of initiatives and any benefit that might derive from them, although a similar project has already been designed (in the private sector) in Italy, as well.

In addition to this, speaking at a teleconference in Tel Aviv, Prime Minister Netanyahu recently announced the forthcoming release of a set of regulations meant to control the export from Israel of cyber security related products. The intention seems to be that of following the same route taken by the USA government: expanding the range of the Wassenaar Arrangement to include technologies and “intrusion software”, useful for general surveillance and hacking purposes. Such arrangement has also been much criticised again earlier this year in the USA by those who ask new changes and more openness for companies. The same kind of debate is presently fueling Israeli political scenario.

**UNITED KINGDOM**

The UK has long since played the leading role in European cyber security and this is not only due to its commitment to combat cyber threats and protect national security but also to the support given for the economic development of cyber security, *i.e.* special terms for businesses active in the field of technology and technological innovation.

This is the background for the new Strategic Defence and Security Review, published on November 23\(^{th}\), 2015, and already become one of the crucial documents to appreciate British Security and Defence Strategy for the next 5 years.

According to the Review, in fact, together with intelligence and counterterrorism, cyber security and notably cyber defence are some of the fields that will see highest investments in the next coming years. About cyber security and cyber defence, this is not surprising. Since the publishing of the first National Cyber Security Strategy, in 2011, the UK’s government indeed invested £860 million in the cyber security field, and over the next five years the UK government will invest £1.9 billion in protecting the country from cyber attack and developing sovereign capabilities in cyberspace. The new strategic document, in fact, refers to ‘cyber threats’, as to one of the four most relevant priorities for the UK government up to 2020.

The Britain’s Strategic Defense and Security Review (SDSR) also pinpoints the next steps of the UK in protecting systems from cyber attacks. These pillars are:

- Develop a series of measures to actively defend UK against cyber attacks (*Active Cyber Defence*).
- Invest in capabilities to detect and analyse cyber threats, pre-empt attacks and track down those responsible.
- Improve the national ability to respond quickly and effectively to cyber attacks. To reach this goal, the UK government will create a new “National Cyber Centre”. This Centre will operate under GCHQ leadership, and will manage the future operational response to cyber incidents, ensuring to protect the UK against serious attacks and minimise their impact.

- Build a new secure, cross-government network to improve joint working on sensitive cyber issues.

- Help companies and the public to do more to protect their own data from cyber threats, providing specialist information. This will include simplifying private sector access to government cyber security advice, and the new “National Cyber Centre” will form a single point of contact for companies seeking advice.

- Create a new intelligence unit dedicated to tackling the criminal use of the ‘dark web’.

- Ensure that the Armed Forces will have strong cyber defences, and that in the event of a significant cyber incident in the UK, they are ready to provide assistance. The government will provide the Armed Forces with advanced offensive cyber capabilities, drawing on the “National Offensive Cyber Programme” run in partnership between the MOD and GCHQ.

- Continue to help NATO and other allies to protect their networks using UK’s intelligence and technical insights.

What emerges from the Strategic Defence and Security Review – also in order to guarantee Italian national security – is the need, strongly highlighted by the British government, to improve the Armed Forces’ cyber defence capabilities and especially to develop excellent and advanced offensive cyber capabilities to help secure UK and NATO’s interests.

This makes the UK one of the fewest countries worldwide and the only one in Europe to have an official policy governing the offensive use of cyber attacks, recalling the strategies adopted by the main international players active and operating in and through cyber space.

In this regard, considerations similar to British ones need to be made urgently by Italian policy makers, at strategic and military level. And this is especially true in light of the new life, high effect and success rates cyber attacks to national critical infrastructures seem to have gained (see Russia and USA paragraphs).

RUSSIA

Few days before the beginning of 2015 Christmas season, Russian government hit the headlines again following the announcement of an alleged implication in a cyber attack organized against some energy infrastructures placed in Ukraine. Last December 23rd, in fact,
the energy companies Prykarpattia OblEnergo and KyivOblEnergo, providing energy to the Western region of Ukraine, publicly claimed to have undergone a cyber attack to the management systems of many of their energy grids, causing a prolonged power outage in a vast area of the region.

Even though it is not the place to analyse the technical details of the event, the curious thing is that the Trojan used to launch the attack is the famous BlackEnergy malware, also used in its first version for the very famous DDoS attacks in Georgia in 2008. In this case, the Trojan infected the system through a fishing attack that carried a Microsoft Word macro and was able to take advantage of a well-known 2014 Office bug, namely CVE-2014-4114. Therefore, an attack not innovative at all but, instead, a very well known and extensively used one.

With an eye to national security, it is interesting that malware developers are paying greater and greater attention to ICS/SCADA systems – especially since 2013. Attacks to critical infrastructures may have physical effects – as is the case with Ukraine – and the growing need for system interconnection – not followed by basic technological security measures nor dedicated regulations – is the weak point of every government.

On the other hand, instead, despite the alleged Russia – Ukraine “cyber war” read on the news, as of now none of the two countries had actually struggled to take advantage of technology and the Internet to launch cyber attacks worthy of being considered as acts of cyber warfare, even less an attack able to directly affect the population, as happened in Ukraine.

Such blackout is indeed to be carefully monitored. Should, in fact, Russian implication be proven (for the moment, it is not), according to international law, such act might at least fall into the “use of force” clause, which, as such, is strictly prohibited by Article 2, § 4, UN Charter, not mentioning all the relevant consequences for Russia, both in its international relations and in case Ukraine decided to counter attack.

UNITED STATES

The USA, as well as China (see relevant paragraph) has publicly announced to be about to start a profound reorganization of its main cyber intelligence agency. The NSA has in fact decided to create a new specialized agency, called Directorate of Operations, enclosing both the Information Assurance Directorate, protecting NSA computer systems and any information thereof, and the Signal Intelligence Directorate, dealing with foreign signals intelligence gathering.
Such a merger is actually following the same route traced one year ago by the Central Intelligence Agency (CIA), which was the first to start merging its cyber space division with the one dealing with analysis of cyber threats.

As usual, the aim of such mergers seems to be rationalizing the huge economic investments in the field of cyber security and increasing as much as possible the effectiveness and efficiency of entities/agencies active in and operating through cyber space, to make them simpler and more responsive.

From the military point of view, thanks to the guarantees set into the chapter “Cyber Operations” of the huge “Law of War Manual”, published in July 2015, U.S. Cyber Command is on the verge of entrusting a project worth over 450 million $ to private contractors with the purpose of receiving support in the next five years while developing the “Cyberspace Operations Support Services”, useful for the Pentagon to project power also in the fifth domain of warfare, the cyber space. To this end, it is the U.S. Cyber Command’s intention to reach 6,200-member unit of Armed Forces specialized in cyber space operations, by the end of 2016.

As a requirement set out in the bid, the winning contractor will be also required to develop and supply cyber weapons in cooperation with USA intelligence agencies. Specifically, according to the draft agreement, the contractor shall give technical support to the US Cyber Command in planning, organising, and coordinating military defensive and offensive activities carried out through the cyber space, as well as advising, developing, assessing and using cyber weapons in such activities.

It is crystal clear that the US government is non-stop working to reinforce its global military and cyber space leadership, and is pushing for a dramatically offensive strategy, already used as a means of deterrence.

Furthermore, this is perfectly in line with the 2017 proposal for financing, submitted by the Pentagon at the beginning of February of this year, with the only cyber security sector requiring 7 billion $ for the next year (about 1 billion more than the request for 2016). In the next five years, additional 35 billion $ are also to be addressed to the protection of military infrastructures and – as explicitly expressed in the request – to speed up the development of offensive capabilities in and through cyber space.

Such request has been followed by the White House Cybersecurity National Action Plan: a strategic document aimed at boosting the federal government’s and the country’s capabilities and strength in the field of computer security by means of specific short-term and medium/long-term activities. To start up such Action Plan, for 2017 President Obama requested 19 billion $: a more than 35% increase in the cyber security budget, if compared to that of 2016.
It is clear that such a strong plan by the White House is the result of the many computer incidents occurred throughout 2015 by means of attacks to the US public administration’s systems (the Office of Personnel Management incident is to be recalled first).

Next month issue will provide a complete analysis of the actions set out in the Cybersecurity National Action Plan.
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 Research Director on “Cyber-security & Cyber-Intelligence” of the Italian Military Centre for Strategic Studies (Ce.Mi.S.S.) of the Italian Ministry of Defense and he is Director of the “InfoWarfare and Emerging Technologies” Observatory of the Italian Institute of Strategic Studies ‘Niccolò Machiavelli’. 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