CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 02 – February 2016

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

Throughout last February, some “emerging” countries in cyber intelligence and cyber warfare activities, such as Iran and North Korea, have been playing a prominent role, once again employing their know-how in this field to pursue their short-term strategic goals. Notably, as diplomatic relations with Saudi Arabia are exacerbating, Iran, the more significantly and fastest growing “emerging country” in this field, might decide to employ its cyber space as the main battlefield.

Through the “*Italian Report on the Security Intelligence Policy 2015*”, Italy has drawn the attention to the first results of the huge attempt made especially by the Intelligence Department to comply with the Italian cyber security regulations and with its cyber-strategy. Nonetheless, three years after their publication, there still seems to be something missing. On the one hand an organic, farsighted agenda, targeted to the creation of an effective Italian cyber security policy is lacking. On the other hand, instead, the Italian government needs to modify its strategic approach toward cyber security, switching from a merely defensive one to a proactive approach.

Finally, the strategic planning effort of the US Government through the "*Cybersecurity National Action Plan*" seems to be very significant. The *Plan* encompasses, in fact, both the reorganization and higher coordination of federal duties in the fields of information security and privacy, and the strong attempt to increase US citizens’ awareness of the problems arising from this field.
Both in the short and medium/long term, the backbone of the US Government in the field is not only to strengthen federal information security and raise the citizens’ awareness, but also to protect their privacy, improve critical infrastructures protection and resilience, design and create “security by design” technological tools. To pursue such policy, investments have been made for 19 billion dollars. And this is a further sign for all the governments that data and information security urgently needs a strategic approach, and actions need to be taken also in the Public Administration, in the short, medium and long term.

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

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

IRAN

Iran's approach to cyber security and cyber warfare can be fully assessed only by describing first the strategic context in which the country operates, as well as the strategic goals it wishes to achieve in the medium-long term.

To this end, Iran's main strategic goal is of being recognized as a regional power. Generally speaking, the country is in fact historically opposed to Saudi Arabia (its main strategic competitor) and the pro-Ryad Gulf Countries, as well as to the USA and Israel.
Actually, the Iranian government does not exactly see the USA as its main enemy, instead it looks forward to being recognized as a regional power first and foremost by Washington.

This is the framework to understand the latest events starring the Iranian government. It is recent news that Saudi Arabia and its allied Gulf Countries interrupted once again diplomatic relations with Iran, following an attack to the Saudi diplomatic mission in Iran – attack very likely arranged by the Iranian government in reaction to sheik Nimr Baqir al-Nimr being sentenced to death and executed by the Saudi government.

Although presently such tensions are very unlikely to give rise to a real Iran-Saudi Arabia conflict – at least in the short period, it is much more likely that the Iranian government resorts to its cyber space as the main battlefield.
After all, Iran is not new at all to this kind of approach and, in fact, in the past it has already played the card of computer attacks in periods of diplomatic crises (see Saudi Aramco and RasGas attacks in 2012). Not to mention cyber espionage activities, propaganda and, in some cases, also computer attacks back in 2015, in order to support its strategic and security priorities, as well as to influence events in its geopolitical area of interest.

To achieve this goals, it is since 2009 that Iran has been investing huge amounts in the development of both its defensive and offensive capabilities, to be employed in case of conflicts and through the cyber space. Already in 2011, in fact, Iran had allocated no less than 1 billion dollars to acquire capabilities aimed at conducting cyber espionage and cyber warfare activities, strengthening and updating its cyber defence section, as well as training personnel to reach such goals. In particular, with President Hassan Rouhani, namely since 2013, Iran has hugely speeded up the pace in this field and can now be considered one of the five main "cyber powers" globally.

After all, also the USA – and not only – have been planning attacks to Iranian computer systems as a possible action to take in case of conflict outbreak. Besides the well-known Stuxnet, it's fresh news that the USA have long been working on a large scale computer attack to be conducted against Iranian airspace, communications and power supply control systems. Nevertheless, the attack program – codename "Nitro Zeus" – seems to be temporarily shelved, following the agreement reached on the Iranian nuclear program.

In light of the above, the continuous and considerable Iranian investments in terms of money, organization efforts and human resources in the field of cyber security and for the development of cyber warfare capabilities make Iran the "emerging" country with the highest and fastest growth in this field.

In this regard, it is important to specify that the Iranian cyber strategy is an integral part of the national doctrine of asymmetric warfare: one of the Iranian cornerstones in conceiving the use of force. The Iranian doctrine, as such, gives a justification – at least in theory – to the country's natural inclination toward offensive activities in and through the cyber space. Moreover, offensive cyber warfare – as well as classical asymmetric warfare (terrorism, guerrilla warfare, etc.) – is considered by the Iranian leadership as an absolutely useful and effective instrument to cause considerable damages to enemies with superior military and technological capabilities.

In the medium term, such a development pattern will lead Iran to play a key international role in geopolitics, similar to that presently played by China but aimed at quickly evolving to become much more similar to that presently played by Russia.

ITALY

As every year, at the end of February the Italian "*Report on Security Intelligence Policy*" (*Relazione sulla politica dell'informazione per la sicurezza*) was presented to the Parliament. The *Report* focuses on the main issues dealt with by the Italian Security Intelligence Department: from jihadi terrorism (and its diffusion in Italy and Europe) to the wave of migration toward the Schengen area; from economic and financial threats to intelligence and criminal attacks, both "traditional" and conducted in and through the cyber space.

The *Report* stresses that, in perspective, cyber threats represent the real "new frontier" for Italian Intelligence agencies and administrations working to ensure national security and even refers to cyber threats as one of the three main challenges for the country together with jihadi terrorism and economic and financial threats.

Furthermore, in 2015 the most important cyber espionage activities to the detriment of strategic national objectives have been conducted as computer attacks against governmental agencies. A continuous increase of acts carried out against governmental agencies and the Italian innovation and technology industry has been observed – both in terms of numbers and quality of the same, with the purpose of obtaining sensitive information and valuable know how, as well as accessing the very same computer systems for future cyber attacks.

Several cases can be numbered as proof of what said above, *i.e.* in economic contexts, where cyber espionage activities are conducted by foreign competitors in order to augment their knowledge of Italian companies. According to the *Report*, such interferences by potential foreign buyers mask secret due diligence aimed at achieving unfair information advantages. Buyers will then use such information in their favour when entering into negotiations to take over Italian economic companies.

What's more, in light of the *Report* of the Italian intelligence Department, the mode of operation of these subjects has turned into an Advanced Persistent Threat (APT), especially featuring the use of malware. Moreover, the attention paid to the "groups" active in APT campaigns showed their inclination from the technical point of view to:

- Employ highly modular malware, equipped with elements carrying out specific functions, to be or not be used according to the target;
- Re-engineer already known *malware*, also contributing to their proliferation, now easily available on the Internet;
- Resort to (when creating a malware code) strings of characters written in different languages or attributable to adversaries, so as to make it even more difficult to determine who launched a computer attack;
- Steal host administrative credentials of the target intranet, in order to keep control of the computer systems even after the systems attacked have been reset and are fully functional;
- Use proxies (both individuals or groups) when conducting computer attacks, to ensure a higher level of anonymity, so that one can deny any kind of involvement even in case the attack is detected.

Finally, the following priorities for the Italian government in the field of cyber security are the result of the analysis carried out in the *Report* by the Intelligence Department:

- Intensifying responses to acts conducted in and through the cyber space;
- Public and private stakeholders to implement the minimum requirements in the field of cyber security;
- Adopting coordinated inter-agency initiatives in the fields of public-private partnership, research and development and international cooperation.

Generally speaking, the Italian *Report on the Security Intelligence Policy 2015* clearly defines and identifies the trend in cyber security. The *Report* draws also attention to the first results of the huge attempt made especially by the Intelligence Department to comply with Italian cyber security regulations, as per Prime Minister's Decree dated January 2013, and with its cyber-strategy.

Nonetheless, three years after their publication, there still seems to be something missing. On the one hand an organic, farsighted agenda, targeted to the creation of an effective Italian cyber security policy is lacking, and this is also due to the absence of basic regulations (*i.e.* a definition of "national security", to inevitably include most of the cyber security related issues).

On the other hand, instead, the comparison with more advanced countries clearly shows that the Italian government needs to urgently modify its strategic approach toward cyber security, switching from a merely defensive one (*i.e.* simple crisis management, adoption of preventative measures against computer attacks and limit of any damages thereof), to a proactive approach, that might help foresee and anticipate trends and future changes in this field, so as to plan in due course any proper action and strategy to be taken.

It goes without saying that all the above cannot and will not be attained without a suitable and committed political support in such a field, by now become essential, so as to allocate as soonest the necessary funds to control such a threat and undertake any action required by its constant and fast evolution.

NORTH KOREA

Last February North Korea has got itself talked about again also for activities carried out in and through the cyber space. Specifically, a wave of low-level computer attacks hit South Korea once again, causing the country to immediately raise the warning level for this kind of threats.

To this end, it is important to highlight that for some time North Korea has been considering cyber space a useful means to reach its purposes of propaganda, intelligence, control of the territory and cyber warfare. This is also due to some characteristics inherent in the cyber domain: asymmetric threats, the possibility to easily deny any responsibility should a cyber attack be discovered, and the high effectiveness of a computer attack compared to the pretty low investments required for its organization and implementation.

In addition to this, in case of counterattacks conducted by opposing countries, North Korea boasts an unrivaled double defence advantage. On the one hand, technology has a very low level of penetration in North-Korean society, and its sensitive national infrastructures are poorly digitalized. On the other, the country can easily disconnect from the Internet, consequently stopping any ongoing computer attack.

Furthermore, it is important to stress that North Korea has always had a preference for asymmetric and unconventional warfare methodologies – both in peace and war times – as a means to tackle the military power of its main enemies: South Korea and the USA. Hence, Pyongyang strategy clearly seems to consist in launching low-intensity unconventional attacks with merely annoying purposes, without ending up being involved in escalations impossible to control or conflicts that would definitely see the country defeated.

As previously mentioned, since 2009 North Korea has considered operations in and through the cyber space as an integral part of its national strategy. To this end it has created within the two most important governmental divisions – the *Reconnaissance General Bureau* and the *General Staff Department* of the Korean People's Army – specific units dedicated respectively to intelligence and cyber warfare.

In light of the above, although in the short term North Korea does not seem to be willing to take the distance from its own strategy, essentially based on low-intensity computer attacks with merely annoying purposes, the mastery acquired time after time in using instruments, the number of successful attacks, as well as the lack of a proper, effective and coordinated response from other countries will soon lead to more frequent and – in the medium term – possibly stronger and higher-quality computer attacks.

TERRORISM: ISLAMIC STATE

Currently the Islamic State is the main terrorist threat for all the Western countries.

Due to the ever-increasing number of European citizens involved in terrorist acts, for a long time experts have been studying more in detail the methods and means used by this terrorist organization to radicalize and shape the thoughts of *shahid*-to-be, despite their being so close to Western principles both by birth and culture, and also distant from religious radicalization areas.

The Internet is one of the most popular and effective means to this end. It is indeed precisely the strategic use of communication through the Internet that the Islamic State has increasingly reduced geographic distances with its supporters, fostering their emotional involvement and adhesion to the principles of jihad and martyrdom.
Actually, the Islamic State has turned technologies and the Internet into the main support instruments to reach its terrorist goals, mostly by way of propaganda, proselytism, radicalization, fund raising and as a first recruitment and indoctrination step.

Nonetheless, despite being considered by the media as capable of conducting significant computer attacks, *i.e.* attacks to national critical infrastructures, or able to create cyber weapons on its own, the organization has never actually raised the bar.

The four main groups supporting the Islamic State, and apparently linked to it, namely the *Cyber Caliphate*, the *Elite Islamic State Hackers*, the *Islamic Cyber Arm*, and the *Islamic State*

Hacking Division, have showed poor capabilities in computer attacks, though. They have simply carried out Denial of Service attacks, defaced websites and social network accounts, and disclosed personal data of government personnel, obtained through basic social engineering techniques.

Instead, what the Islamic State is more focused on is finding the most secure methods and means of communications possible.
It is in fact by using the Internet as a crucial means to recruit new supporters that in some cases some of the key subjects involved in the jihadi propaganda have been identified, geolocated, and even killed, due to the high levels of exposure. This is the case with Junaid Hussain, also known as Abu Hussain al-Britani, born in Birmingham and leading member of the *Cyber Caliphate*, located and killed by an American drone last August 2015, in Raqqa, Syria, also as a result of the "traces" left of his on-line activity.

Once again, although propaganda and then the media depict the Islamic State as capable of developing software completely securing communications among the members of the terrorist group – as in the recent case with the mobile app called *Alrawi* – there is actually no trace on the Internet of such software nor of the *Alrawi* app. On the contrary, all the information available in the field of secure communications leads to believe that the popular mobile app Telegram is also used by the Islamic State. All the rest is merely propaganda.

Based on the information above, Islamic State capabilities of conducting computer attacks for terrorist purposes are not deemed to be significantly evolving in the short/medium term, compared to the situation described above. Consequently, the level of danger of such threat in Western countries can be still considered as very low.

In addition to this, although the Islamic State seems to be seriously considering the idea of recruiting computer engineers and computer security specialists (also drawing from Anonymous activists), the main concern for the West comes exclusively from some countries close to the terrorist organization, likely to start supporting Islamic State activities also in the cyber space.
This is something that might occur even in the short period either through financing (even if it is important to point out that it is unlikely that such funds will be actually used by the Islamic State to raise its offensive capabilities in and through the cyber space), or – and it is instead more likely – should such countries provide the IS with software and know how useful to conduct computer attacks to a country's critical infrastructures.

Nevertheless, should such scenario come true, the level of danger for Western countries would still be considered as medium-low, due to the almost certain lack of time continuity of the attacks. Furthermore, for the "financing" country, such attacks would exclusively aim at reiterating the well-known practice of a computer attack conducted by resorting to a non-state actor as a proxy.

UNITED STATES

As mentioned in the last volume of the *Cyber Strategy & Policy Brief*, in early February the White House has published its "*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. Highlights of the *Cybersecurity National Action Plan* include actions to:

- Establish the *Commission on Enhancing National Cybersecurity*. This *Commission* will assemble twelve leading cybersecurity and privacy experts from across the private sector to make recommendations on actions that can be taken over the next decade to strengthen cybersecurity in both the public and private sectors while protecting privacy, and maintaining public safety and economic and national security of the United States. Furthermore, the *Commission* will foster the discovery and development of new technical solutions, and will bolster partnerships between Federal, State, and local government and the private sector in the development, promotion and use of cybersecurity technologies, policies, and best practices.
- Modernize Government IT and transform how the Government manages cybersecurity through the proposal of a $3.1 billion Information Technology Modernization Fund. The Administration will also create – for the first time – the position of *Federal Chief Information Security Officer* to drive cybersecurity policy, planning, and implementation across the Federal Government.
- Empower Americans to secure their online accounts by moving beyond just passwords and adding an extra layer of security. This focus on multi-factor authentication will be central to a new *National Cybersecurity Awareness Campaign* launched by the *National Cyber Security Alliance* in partnership with leading technology firms like Google, Facebook, DropBox, and Microsoft to make it easier for millions of users to secure their online accounts, and financial services companies such as MasterCard, Visa, PayPal, and Venmo that are making transactions more secure.
- The establishment of a Federal Privacy Council, composed of representatives from various key federal agencies, to coordinate guidelines for the federal government's collection and storage of data.

Finally, the strategic planning effort of the US Government through the "*Cybersecurity National Action Plan*" seems to be very significant. The *Plan* encompasses, in fact, both the reorganization and higher coordination of federal duties in the fields of information security and privacy, and the strong attempt to increase US citizens' awareness of the problems arising from this field.

Both in the short and medium/long term, the backbone of the US Government in the field is not only to strengthen federal information security and raise the citizens' awareness, but also to protect their privacy, improve critical infrastructures protection and resilience, design and create "security by design" technological tools. To pursue such policy, investments have been made for 19 billion dollars.

This is a further sign for all the governments that data and information security urgently needs a strategic approach, and actions need to be taken also in the Public Administration, in the short, medium and long term.

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