CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 11/12 – November/December 2016

EXECUTIVE SUMMARY

Keywords: *China, Critical Infrastructures, Cyber Attack, Cyber Command, Cyber Security, Cyber Strategy, Governance, India, Iran, Law, OPEC, Saudita Arabia.*

Despite hugely moving ahead with modernization and digitalization of its national infrastructures and relative procedures, **Saudi Arabia** still seems backward in its capacity to ensure high cyber security standards for its main strategic assets, turning out to be the main target of cyber-attacks in the Middle East still now.

The recent wave of cyber-attacks undergone last mid-November by several Saudi governmental agencies is in fact a confirmation of what just said, with agencies included such as the Central Bank, the Ministry of Transportations and the General Authority for Civil Aviation, forced to stop their activities for some days further to massive cancellation of the data necessary to operate their information systems.

The analysis of the information available up to now shows that it is quite unlikely what most of the analysts and the media currently maintain: directly pointing at **Iran** once again. It is much more likely, instead, that an attack has been carried out by groups supported by the Iranian government or someway linked to other countries opposing the Saudi government. Such individuals, in fact, might want to check abilities and highest capabilities of Saudi Arabia and its main public and private entities, so as to cause limited political and economic damages in the short term, and especially acquire valuable information for possible future warfare in and through the cyber space.

Moving to Southern Asia, instead, at the beginning of December, rumors from the media had it that a forthcoming first **Indian Cyber Command** was about to be established, aimed at unifying and focusing the efforts of the single Armed Forces to counter and mitigate in the best possible way the even more persistent threats to national security coming from cyberspace.

Although such a project has been in the pipeline since 2010, time does not seem to be ripe yet and implementation of this paramount goal – that would bring India in line with the other main countries both in the region and globally – inexplicably seems to be postponed once again.

The lack of an holistic approach to the issue of cyber security, able to put together the efforts carried out by single institutional players and the private sector so as to outline a coherent institutional architecture that is in line with the goals, undoubtedly represents the main field in

which the Indian government is required to take action nowadays as a matter of urgency and especially with a long-term perspective.

Finally, this issue also focuses on the **new Chinese political, strategic and regulative approach to cyber security**.

Understanding Chinese goals and capabilities in the field of cyber security represents an urgent matter so as to fully gather Asian stability, as well as to have an overview on international policy, in light of Chinese ambitions to widen the country's sphere of influence to the whole world.

The focus is then on both the **first People's Republic of China's Cyber Security Law** and the **new national cyber security strategic document**.

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

CHINA – FOCUS ON THE NEW POLITICAL, STRATEGIC AND REGULATIVE APPROACH TO CYBER SECURITY

China's goals and capabilities in the realm of cyber security represent a pressing issue for understanding Asian stability and, as Beijing expands its sphere of influence worldwide, also for international politics more in general. While the assessment of China's capabilities remains complicated and controversial even among experts, two recent documents shed light on China's goals and interests in this realm.

At the end of last year, China has in fact published two crucial documents on its cyber security policy. On November 7th, 2016, the Chinese government officially adopted its first law completely focused on cyber security, while just before the end of the 2016 it released the new national strategic document for cyberspace security.

The first "Law of the People's Republic of China on Cyber Security"

As far as the "*Law of the People's Republic of China on Cyber Security*" is concerned – entering into force next June – the aim declared in Article 1 is to guarantee network security in order to safeguard cyberspace sovereignty, national security and social interests, but also to protect the lawful rights and interests of citizens, legal persons and other organizations, as well as to promote economic and social development through technology.

Nevertheless, by reading the law in full, it can be highlighted that the whole regulatory pattern, as set by the Chinese legislator, actually aims at strengthening – resorting to the law – the Beijing government's possibility and capability to control its citizens, and public and private actors operating on the territory of People's Republic of China.

What's more, the regulation does nothing else but crystallizing duties and prohibitions, already informally in force, for both citizens and operators providing IT products and services.

In this view, by way of example, Article 12 expressly prohibits – inter alia – each person and organization from using the networks to prejudice Chinese honor or national interests, it also prohibits to encourage subversion of national sovereignty or overthrow of the socialist system or to spread forged information aimed at undermining economic and social order.

Talking about public and private actors, instead, despite the valuable effort made by the Chinese legislator to implement within the very same law some "minimum" security measures for network operators (Article 21) and for companies that can be classified as critical information infrastructures (Article 34), to which one or more of the seven "*Cybersecurity and Data* *protection National Standards*" currently undergoing public consultation – according to the interested field – shall be added, some doubts arise when looking at other articles of the law.

For instance, this is the case with Article 23, prohibiting the sale and supply of network equipment or network security products unless they are inspected and certified by a governmental agency attesting their compliance with the requirements of the Chinese law and national security standards.

This is also the case with Article 37 – one of the most controversial – requesting companies that can be classified as critical information infrastructures to store within mainland People's Republic of China all the personal data and any other relevant information gathered or produced in China while carrying out their activities. Furthermore, in case for grounded business reasons such data and information should be sent abroad, the security levels of these very same companies shall be evaluated by specific State entities.

As it's easy to notice, the approach of the Chinese Government is particularly strict, and basically follows the approach of many other countries such as Russia or Iran, as pointed out in May 2016 *Cyber Strategy & Policy Brief*.

Article 58 also raises some doubts in it directly assigning to the State Council or to Chinese governments of provinces, autonomous regions or municipalities – upon prior approval of the State Council – the possibility to temporarily limit IT communications, should it be necessary to protect national security, public order or to counter serious security incidents affecting citizens.

Finally, Article 75 specifies that, should foreign entities, organizations or individuals carry out attacks, intrusions, interferences, damages or other activities that may jeopardize Chinese critical information infrastructures, causing serious consequences, the Ministry of Public Security and other governmental entities in charge shall not only be legally responsible but might also decide to freeze the assets or adopt further not better specified punitive measures.

After reading on the whole the first "*Law of the People's Republic of China on Cyber Security*", although the Chinese legislator' significant and valuable effort is clearly intended to organize and harmonize the whole field of cyber security within a single law, some concerns cannot be left out on those provisions evidently aimed at ensuring the Chinese government a strong domestic control on all the activities conducted in and through the cyberspace by citizens, and both national and international public and private operators.

The new National Cyber Security Strategy

Published on December 27th, 2016, the new Chinese cyber security strategy is mainly focused on two strategic goals strictly connected with the above-mentioned "*Law of the People's*

Republic of China on Cyber Security", namely safeguarding cyberspace national sovereignty and protecting national critical information infrastructures.

The safeguard of cyberspace national sovereignty is in fact the first and most relevant strategic pillar for the Chinese government within the document, at such a point that the will to safeguard it is explicitly declared, in open opposition to any attempt to use the Internet to overturn the Chinese national regime or to sabotage its sovereignty on the territory. To reach such a goal, Beijing also maintains that it is ready to use whatever means considered necessary, be it scientific, technological, legal, diplomatic or military.

The second pillar, dealing with the protection of national security, must be read together with the previous one. In this case, the objective is to anticipate, repress and punish, as provided for by law, a series of behaviors that are well defined in the strategy, namely:

1. Any attempt whatsoever to use the Internet for treason, separatism, incitement to rebellion, subversion or overthrow of the People's democratic dictatorial regime.
2. Any attempt whatsoever to use the Internet to steal or leak state secrets or to conduct other similar actions aimed at harming national security.
3. Any attempt whatsoever made by foreign countries to use the Internet for infiltration, destruction, subversion and separatist activities.

The second predominant strategic goal of this new cyber security strategy is to protect Chinese critical information infrastructures.

Yet, both the previously mentioned law and the new strategy give a very wide and, most of all, too general definition of critical information infrastructure, encompassing any structure affecting national security, the Country's economy as well as the livelihood of its citizens.

In addition, the strategy analyses in depth many preventive cyber security activities exclusively aimed at protecting such structures, focusing attention on two elements:

1. Protection of critical information infrastructures by strengthening the following procedures: user identification, early warning, prevention and monitoring of attacks; and
2. Development of deterrence to attack by increasing the security of critical information infrastructures.

In addition – in line with what provided for by Article 23 of the law examined above – the Chinese government reaffirms its intention to prevent governmental bodies from using technology products and services in the absence of prior inspection and certification by a governmental structure attesting their compliance with the provisions of Chinese law and with national security standards.

Finally, the strategy also provides for further surely relevant objectives, such as, by way of example, strengthening online anti-terrorism, counterespionage and anti-theft capabilities – activities that are only mentioned but not specifically dealt with – or gathering the efforts to perfect national network governance systems especially by promulgating laws (as the one just examined), or even strengthening international cooperation resorting to the United Nations and signing bilateral and multilateral agreements on cyber security.

To conclude, the joint analysis of the new strategy and the first cyber security law shows that the Chinese approach is clearly aimed at safeguarding first of all its political leadership, monitoring and, in case of need, slowing down information and propaganda activities conducted in and through the cyberspace mainly by national opposition parties and by political and social dissident groups.

Meanwhile, the Government is also undeniably interested in affirming and strongly safeguarding national sovereignty in cyberspace security, as well as enhancing protection and defence levels of its critical information infrastructures

Some strategic priorities can then be identified, definitely similar to those already outlined in previous Chinese cyber strategies. Yet, it is understood that Beijing does show a greater maturity and openness to see international cooperation as an essential element for cyber security and for the development of Chinese economic interests and geopolitical ambitions.

INDIA

At the beginning of December, as happens cyclically lately, rumors from the Indian media had it that a forthcoming first Cyber Command was about to be established, aimed at unifying and focusing the efforts of the single Armed Forces to counter and mitigate in the best possible way the even more persistent threats to national security coming from cyberspace.

Although such a project has been in the pipeline since 2010, time does not seem to be ripe yet and implementation of this paramount goal – that would bring India in line with the other main countries both in the region and globally – inexplicably seems to be postponed once again.

This, moreover, despite the late re-exacerbation of India-Pakistan tensions has more than once resulted in waves of cyber attacks whose targets were Indian governmental systems.

After all, with more than 460 million Internet users in 2016, which equals the 34.8% of its population, and around 100 million new users every year, India cannot and has never ignored the problem of cyber security.

Notwithstanding, this country currently seems to be particularly backward if compared to other countries in political and strategic planning in this field, especially when it comes to the implementation of the provisions of its 2013 cyber strategy.

The 14 strategic pillars of Indian *National Cyber Security Policy* – issued in 2013 and not updated yet – had in fact set the grounds in a correct and forward-looking way for the development of this field, namely national security, contrast to criminality, and increased knowledge of such issues for the citizens. Nevertheless, after three years, the implementation of this Policy still seems very far from reaching most of the above-mentioned goals.

In addition to this, not even the appointment of a National Cyber Security Coordinator on December 2014 could reach the expected political turning point. In fact, despite the valuable efforts carried out so far to tackle cyber crime, that right speedup in the reform process is still lacking together with a role as institutional link suggested by the Indian cyber strategy and essential to face up to cyber threats effectively and efficiently.

To conclude, the lack of an holistic approach to the issue of cyber security, able to put together the efforts carried out by single institutional players and the private sector so as to outline a coherent institutional architecture that is in line with the goals, undoubtedly represents the main field in which the Indian government is required to take action nowadays as a matter of urgency and especially with a long-term perspective.

SAUDI ARABIA

Despite hugely moving ahead with modernization and digitalization of its national infrastructures and relative procedures, Saudi Arabia still seems backward in its capacity to ensure high cyber security standards for its main strategic assets, turning out to be the main target of cyber attacks in the Middle East still now.

On the one hand, in fact, the ambitious aim of the recent "*National Transformation Program 2030*" is to create a long-term, real, cutting-edge digital ecosystem, active in all the 24 governmental agencies involved in Saudi economic development. To this end, the government intends to invest 268 billion Riyal (over 66.5 billion Euro) in the first five years of program implementation. Nevertheless, on the other hand, the Saudi government still seems to be highly backward in cyber security, from the technical, legal, policy and especially strategic standpoints.

The recent wave of cyber attacks undergone last mid-November by several Saudi governmental agencies is in fact a confirmation of what just said, with agencies included such as the Central Bank, the Ministry of Transportations and the General Authority for Civil Aviation, forced to stop their activities for some days further to massive cancellation of the data necessary to operate their information systems.

Although the information available is still very limited, the companies that have examined the malware used (*Disttrack Wiper* – W32.Disttrack.B) have highlighted its evident similarity with *Shamoon*: the malware probably used by Iran in 2012 to hit some Saudi companies active in the energy field – such as Saudi Aramco – that, even in that case, canceled the critical data necessary to operate information systems.

Such a similarity in objectives and means, together with the constant diplomatic tensions between Saudi Arabia and Iran, have led most of the analysts to point at the Iranian government once again.

After all, as examined in detail in February 2016 *Cyber Strategy & Policy Brief*, it is a long time since Saudi Arabia and Iran have been resorting to an equivalent retaliation strategy (also known as "*Tit-for-Tat*"), employing also cyberspace as a provocation or reaction tool.

The February issue, in fact, anticipated that, following the umpteenth interruption of diplomatic relations between the two countries, it was likely that the Iranian government could resort to its cyberspace as the main battlefield against Saudi Arabia in order to prevent excessive escalation.

Nonetheless, in light of the limited information currently available, such a preliminary examination phase cannot exclude *a priori* other theories.

Hence, it might as well be likely that third parties – almost certainly State actors or State-supported actors – simulated a cyber attack coming from Iran to try and jeopardize Iran-Saudi Arabia relationships in the lead-up to the deal to reduce daily crude oil production – the agreement was then actually signed by Saudi Arabia and Iran at the 171st meeting of the Organization of the Petroleum Exporting Countries (OPEC).

The following must be specified on this theory, though.
First, such a cyber attack – what's more conducted against only one of the actors involved – would have unlikely undermined Saudi Arabia-Iran diplomatic relationships at such a point to make a deal on such a relevant matter fall through. As a confirmation of the above, the agreement has been reached in any case, despite what happened.

Secondly, instead, it seems difficult to find a third State that is not only prepared to conduct coordinated cyber attacks on several medium-high level Saudi targets, but is especially able to take advantage from the desired failure for the governments of the two countries to reach an agreement.
Yet, an analysis of the scenario shows that United States, Russia and the other main players having both these features shall all take economic advantage from such a deal. This, in fact, makes a possible motive fail and the above-mentioned theory, maintained by most of the international media, sway even more.

Talking about further theories, the possibility that an attack has been carried out by groups supported by the Iranian government or someway linked to other countries opposing the Saudi government might be likely as well. Such individuals, in fact, might want to check abilities and highest capabilities of Saudi Arabia and its main public and private entities, so as to cause limited political and economic damages in the short term, and especially acquire valuable information for possible future warfare in and through the cyberspace.

To conclude, setting aside those who are really behind this last wave of cyber attacks, the overall analysis of the strategic and political activities carried out up to now by the Saudi government clearly shows that the several and huge economic investments Saudi Arabia has made actually lack a strategic and regulatory connection, able to play a fundamental boosting role for the public and private sector, as well as linking them in view of a mutual cooperation.

Although the Saudi government's 2013 *National Information Security Strategy* clearly stressed the need to make up for such flaws, presently the advice above still seems to be far from being implemented.

This led the main public and private Saudi actors to develop protection systems and cyber security initiatives on their own and in a non-coordinated manner, only after being the target of a cyber attack.

It is indeed desirable that Riyadh focuses at soonest its efforts on the merely technical aspects of cyber security, as well as on its legal, policy and especially strategic aspects, in order to support its great economic commitment with a clear and pragmatic strategic vision to be of help to the whole sector.

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 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.*

Cyber Strategy & Policy Brief (Volume 06 – June 2016)

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.*

Cyber Strategy & Policy Brief (Volume 07/08 – July/August 2016)

Keywords: *Cyber Warfare, Rules of Engagement for Cyberspace, FBI, DHS, ODNI, United States.*

Cyber Strategy & Policy Brief (Volume 09 – September 2016)

Keywords: *Cyber Warfare, Department of Homeland Security (DHS), Elections, Electronic Voting Systems, Espionage, Influence Activities, Information Warfare, International Law, Offensive Cyberspace Operations, Office of the Director of National Intelligence (ODNI), Propaganda, Russia, United Nations, United States.*

Cyber Strategy & Policy Brief (Volume 10 – October 2016)

Keywords: *Association of South-East Asian Nations (ASEAN), Critical Infrastructures, Cyber Crime, Financial Sector, G7, National Security, Risk Analysis, Singapore, Strategy, Turkey, United States.*