CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 09 – September 2016

EXECUTIVE SUMMARY

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.*

This volume of the "*Cyber Strategy & Policy Brief*" is completely focused on U.S.-Russia political tensions in the wake of the upcoming presidential elections.

The Russian Government, in fact, is alleged to conduct influence activities intended to interfere with the U.S. election campaign, especially by illegally stealing and then publishing online private emails and confidential information from Democratic National Committee.

One additional suspect is that the Russian Government is also regularly conducting remote scanning and probing of some U.S. States' election-related information systems. This, in order to verify their security level, try to interfere with their functioning and consequently the results.

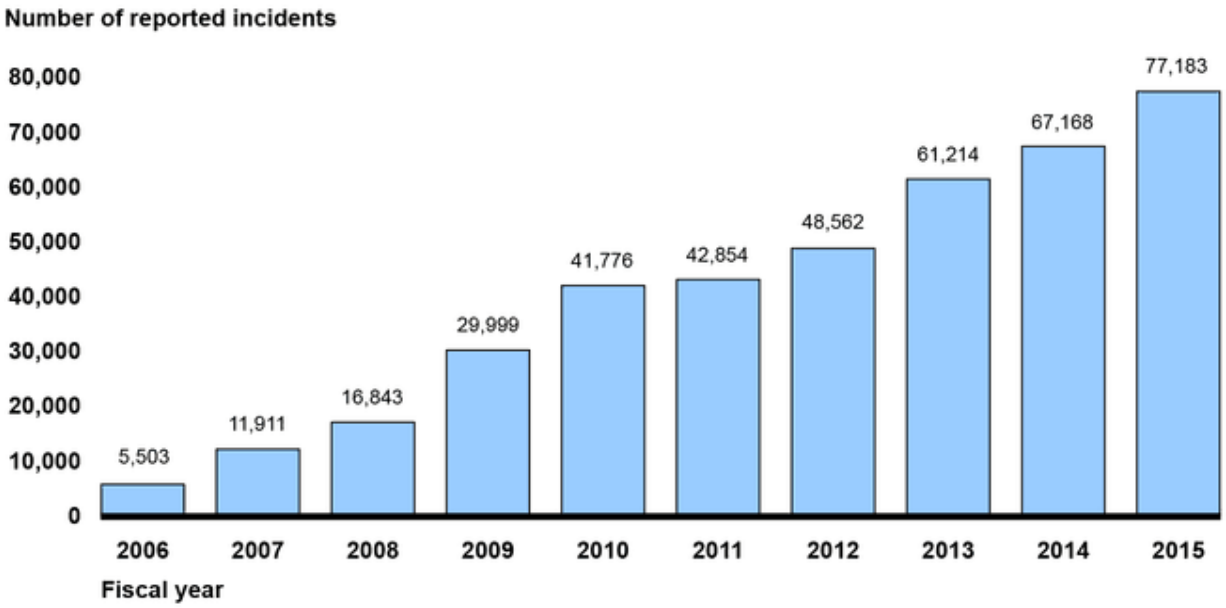
Therefore, this *paper* analyses:

- U.S. formal accusations to Russia.
- The Russian strategy.
- The U.S. strategy.
- Issues concerning U.S. reaction.
- Electronic voting systems protection strategy.
- U.S. possible responses to Russian activities.

FOCUS ON U.S. ELECTIONS AND U.S.-RUSSIA POLITICAL TENSIONS

The U.S. are still one of the main targets for cyber attacks conducted by primary international players, being they State actors or State-supported actors, criminal organizations, terrorist groups or merely activists.

According to recent official reports, cyber incidents affecting U.S. federal agencies have endured a staggering 1,300 percent rise in the last ten years. In 2015, in fact, 77,183 incidents have been reported against 5,503 reported in 2006.



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-885T

Looking at the recent events, it is clear that threats are finding more easily (and effectively enough) their way in the fields of propaganda, disinformation, information manipulation and espionage thanks to cyberspace.

As also pointed out in March 2016 *Cyber Strategy & Policy Brief*, the present incapability to deter, together with the difficulty in coordinating roles, competences and responses to cyber threats helps creating a more and more troubling and complicated international scenario.

U.S. formal accusations to Russia.

It is under this scenario that the U.S. Department of Homeland Security (DHS) and Office of the Director of National Intelligence (ODNI) have recently formally accused Russia.

In the wake of the upcoming presidential elections, in fact, the Russian Government is alleged to conduct influence activities intended to interfere with the U.S. election campaign, especially by illegally stealing and then publishing online private emails and confidential information from Democratic National Committee.

One additional suspect is that the Russian Government is also regularly conducting remote scanning and probing of some U.S. States' election-related information systems. This, in order to verify their security level, try to interfere with their functioning and consequently the results.

The Russian strategy.

The Russian Government is not new at all to this kind of activities, though. It was in fact accused to conduct massive information influence, propaganda and cyber attacks aimed at breaching electronic voting security systems or leaking confidential information to be then disclosed online – in an attempt to influence the presidential campaign in Ukraine back in 2014.

However, this type of activities are to be set not only in the specific historical moment in which they take place – as is the case with the U.S. presidential elections – but also in the wider Russian strategic approach, always aiming to spread uncertainty and destabilize the institutions of enemy countries by means of influence activities, interference, disinformation and information intoxication. The Russian strategy, in fact, is mainly based on influence and not on force. It is therefore intended to undermine internal cohesion of Governments and not totally destroy them.

The U.S. strategy.

The U.S. Government political and strategic purpose of such direct accusations is indeed specific enough.

By starting accusing – in a direct and formal way – the real authors of State or State-sponsored cyber crimes, first the U.S. Government intends to publicly demonstrate their capability to trace back the authors of those attacks.

This means sending worldwide the message that they are able to solve the main problem in the field of cyber security, which is anonymity and incapability to find the real authors of cyber attacks in a reasonable time and for certain. This, also in order to deter adversary and allied countries from conducting such attacks.
Also, acquiring such a capability is a further key element to contribute filling one of the primary "voids" so as to strengthen a truly consistent and effective cyberspace deterrence strategy.

As a matter of fact, the U.S. have adopted such a strategy since a long time, as already detailed in March 2016 *Cyber Strategy & Policy Brief*. Back in May 2014, in fact, the U.S.

Department of Justice formally charged five members of the Chinese People's Liberation Army (PLA) 'Unit 61938' with cyber espionage for breaching the information systems of six U.S. companies in search of industrial secrets.

Moreover, at the beginning of 2016, the U.S. Department of Justice also unsealed indictments against a group of seven Iranian citizens employed in two private companies working for Teheran Government and its Islamic Revolutionary Guard Corps, for conducting a coordinated campaign of terrorist attacks against U.S. financial institutions between 2011 and 2013. An additional charge has been filed against one of the seven Iranian hackers for illegally accessing the command and control information systems of a dam in New York.

Issues concerning U.S. reaction.

Nevertheless, although on one hand the advantages of this reactive approach to cyber attacks undergone seem evident, on the other hand these public accusations have not so insignificant consequences for the U.S..

First, from the legal standpoint, it needs to be stressed that the U.S. Government was one of the principal promoters and signatories of the 2015 United Nations Governmental Experts Report. This latter, in fact, clearly states that the accusation of organizing and implementing wrongful acts against States should be substantiated.

Nonetheless, should the Russian Government implication be proved, the U.S. would publicly reveal their intelligence capabilities towards Moscow, and almost surely not only in the field of cyber security. Yet, once obtained such information, the Russian Government could easily find and quickly fix their flaws and weaknesses, thus undermining U.S. intelligence capabilities.

President Obama shall also face challenging decisions to adopt when it comes to the reactions threatened to take against Russian cyber attacks.

As per military policy, the U.S. Government has several options to choose from, though.

In fact, even though the U.S. have started designing and organizing their forces for information warfare and cyber warfare after the First Gulf War in 1991, the use of cyberspace for operative military purposes was made official only in 2004, a time when the then National Military Strategy explicitly set forth that "*the* [U.S.] *Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains*." The same concept then evolved in 2006 Quadrennial Defense Review, for the first time announcing that the U.S. DoD would consider cyberspace as a new warfare domain.

What's more, declassifying 2013 Joint Publication 3-12 military doctrine for Cyberspace Operations has clearly shown that the Pentagon has started to formally recognize and is using military offensive activities intended to "*project power in and through cyberspace*" in order to "*degrade, disrupt or destroy access to, operation of, or availability of a target by a specified level for a specified time*" or to "*control or change the adversary's information, information systems or networks*" (such activities are also called "Offensive Cyberspace Operations" or OCO).

To conclude, a further, highly relevant statement is to be added: the one contained in 2011 International Strategy for Cyberspace, in which the U.S. reserve their right to respond to hostile acts in or through cyberspace relying on any necessary means: diplomatic, information, military and economic ones. Hence, this implies responses to cyber attacks undergone may also be conducted by means of conventional military operations.

Nevertheless, this kind of provisions and, in practice, military operations are still today open to relevant (especially legal) issues that are quite far from being solved.

It is in fact undisputed that the international law in force applies also to the States' conduct in cyberspace. *Inter alia*, the fundamental principles of humanity, proportionality and distinction are always to be kept in consideration, especially in case of a military reaction to an attack.

In any case, complying which such legal principles and keeping under control the escalation of a cyber attack is not that easy and immediate presently.

Electronic voting systems protection strategy.

A new element of this strategy is to secure electronic voting systems, that are being more and more targeted by cyber attacks, as U.S. presidential ballot-casting approaches.

Indeed, five U.S. States – Delaware, Georgia, Louisiana, South Carolina, and New Jersey – totally rely on electronic voting, while a mixed voting system is in use in other ten States.
In light of this, the low security level of such systems and also lack of the opportune post-election polls on coherence of ballot casting might involve the concrete risk to see the results of voting process rigged due to a cyber attack.

To this end, on September 20th, 2016, the U.S. House of Representatives proposed two bills specifically aiming at mitigating this risk.

Namely, the purpose of the first one – "Election Infrastructure and Security Promotion Act of 2016" – is to request the U.S. Department of Homeland Security (DHS) to designate this kind of information systems as national critical infrastructure, as already happens with electrical,

energy and hydraulic systems, telecommunication networks and public transportation, banking and financial networks, and so on.

Instead, the second bill, "Election Integrity Act of 2016", *inter alia* aims to limit the acquisition of electronic voting systems that do not produce a voter-verified paper record.

Although both these bills clearly seem belated for U.S. forthcoming presidential elections, they obviously aim to open future federal investments to make the electronic voting system more secure.

Nonetheless, designating electronic voting systems as U.S. national critical infrastructures first of all implies qualifying cyber attacks as high-profile cyber threats, namely those likely to "*result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people*", as recently defined within Presidential Policy Directive No. 41 "*United States Cyber Incident Coordination*" (for details, please see February and July/August 2016 "*Cyber Strategy & Policy Brief*").

The U.S. might then want to give a harder response to this kind of attacks, that is especially more coordinated not only with regard to cyber, but also from a diplomatic and economic standpoint and even, as mentioned above, by resorting to kinetic military operations.

U.S. possible responses to Russian activities.

Beyond any possible illicit operations to be conducted in and through cyberspace, all the above shows that a possible public response from the U.S. Government to Russia might once again take the typical form of diplomatic and economic reactions, and military support to the countries adjoining Russian borders.

One first option might be then to resort to economic sanctions under April 1st, 2015 Presidential Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities".

According to this Executive Order, in fact, properties and bank accounts in the U.S. that can be attributable to Putin and other Russian leaders close to the President might be frozen.

This possibility is not very new, though. Back in 1999, in fact, the White House preliminary approved a very similar plan to hit and drain foreign bank accounts of the then Serbian leader Milosevic and his supporters. In 2003 as well, the U.S. designed a similar project before Iraq second invasion, targeted to hit Saddam Hussein's financial system.

A second option, instead, might be to disclose the conversations proving that Russian Government was involved in the cyber attacks conducted against the National Democratic Committee servers and electronic voting systems.

Making public the names of the politicians or officials that personally gave authorization to conduct such cyber attacks not only would mean providing evidence to the accusations raised by the White House, but would surely compromise Moscow worldwide.

Nevertheless, as mentioned above, all of this should not expose U.S. intelligence capabilities too much, so as to prevent Russia from catching U.S. security leaks or the sources used.

Finally, a last option might be to publicly disclose Russian internal control methods and systems used to monitor contents published online and activities carried out on the Internet by Russian citizens. This, in order to undermine the internal stability of the Government in charge and President Putin's leadership, moreover by resorting to activities that are very similar to those suffered by the U.S..

Whatever the option actually chosen, any of these activities has to be carefully considered and arranged in detail, in order to avoid an escalation difficult to manage. After all, it seems undisputed to maintain that the election of the new U.S. President shall help such skirmishes fade even in the short term, although a complete solution to the problem will not be reached.

Beyond the case *per se*, it is indeed clear that a protracted inaction and the fact that Governments decision-making times are very slow worldwide, together with the constant incapability to find simple answers to cyber threats are quickly leading to an exponential and almost unmanageable increase of cyber attacks backing information influence, espionage and cyber warfare.

Designing and implementing agreements including confidence-building measures is something to be urgently thought about, so as to avoid any possible arms race and recognize limits in terms of targets and tools to be used.

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*.

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.*