CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 07/08 – July/August 2016

EXECUTIVE SUMMARY

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

The number of cyber attacks is constantly growing not only in quantity, but especially in quality, considering both the targets being hit, and the complexity and actual objectives of such attacks.

Even leaving out for once cyber espionage threats and cyber warfare, recent news, for instance, clearly show it is long time since propaganda, disinformation and psychological warfare have "made their way" – very effectively, though – thanks to cyberspace, that has by now become one of the main players, also trying to influence the campaign for U.S. elections.

The poor capability to deter (for more details, please see March 2016 "*Cyber Strategy & Policy Brief*"), together with the incapability in coordinating roles, competences and responses to cyber threats, contribute to create a clearly troubling scenario.

To this end, and on the wake of what set forth in the "*Cybersecurity National Action Plan*", published last February (for more details, please see February 2016 "*Cyber Strategy & Policy Brief*"), the recent *Presidential Policy Directive* by President Obama – also known as "PPD-41 - *United States Cyber Incident Coordination*" – is of great interest and spells out the lines of responsibility within the federal government for cyber incident response.

The goal of such restructuring is to create a plan to coordinate roles and concentrate efforts, acting through a *Cyber Unified Coordination Group* able to face significant cyber threats that – for dimension, nature or intensity – might undermine U.S. national security and the security of its citizens.

This is a very challenging objective, that – nonetheless – by now proves to be useful and essential, especially in really complex structures, as is the case with U.S., but that is waiting to be examined after entering into force and being effectively implemented.

This month, the focus is on the rules of engagement for cyberspace.
Although military operations in and through the cyberspace by now play an essential role especially in facilitating the Armed Forces' conventional attacks, the rules of engagement remain secret in most of the cases and represent one of the less discussed subjects in the field of cyber security (and not only).

This is mainly due to the fact that – generally speaking – the rules of engagement aim to identify and define the events and limits within which the Armed Forces can start and/or continue fighting against opposing forces, setting the standards for authorized and non-authorized behaviors to adopt or not to adopt in the presence of particular hostile activities or actions.

As already said, this implies a great need for secrecy on contents. Rules of engagement for cyber space obviously make no exception.

Arranging rules of engagement for cyberspace presently looks like a particularly complex activity, the outcome of a mix of military, legal, technical and technological competences that are not so easy to be understood and implemented.

Nonetheless, the more and more widespread use of cyberspace as a support tool to military operations and the constant growth in number and quality of cyber attacks – more and more focused on hitting national critical infrastructures – make this need highly topical and absolutely not deferrable, now more than ever.

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

FOCUS ON RULES OF ENGAGEMENT FOR CYBERSPACE

Last June 14th, the Ministers of Defence of NATO countries recognised cyberspace as the fifth warfare domain, after land, sea, air, and space. A formal official statement then followed at the 27th NATO summit of the heads of state and heads of government held in Warsaw at the beginning of July (for further details, please also see June 2016 "*Cyber Strategy & Policy Brief*").

Nevertheless, it is long since almost all the main countries have created dedicated structures to tackle cyber threat, both at a governmental level and in the field of intelligence and military operations.

Although it is quite difficult as of now 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. And the figure goes up to 100 countries, including those about to develop them.

In this field, although military operations in and through the cyberspace by now play an essential role especially in facilitating the Armed Forces' conventional attacks, the rules of engagement remain secret in most of the cases and represent one of the less discussed subjects in the field of cyber security (and not only).

This is mainly due to the fact that – generally speaking – the rules of engagement aim to identify and define the events and limits within which the Armed Forces can start and/or continue fighting against opposing forces, setting the standards for authorized and non-authorized behaviors to adopt or not to adopt in the presence of particular hostile activities or actions.

As already said, this implies a great need for secrecy on contents. Rules of engagement for cyber space obviously make no exception.

Notwithstanding, rules of engagement are often contained in documents that are as brief as complex.

In the field of military operations in and through the cyberspace, they include legal, strategic, operative and tactical elements, all of which are based on a deep knowledge and examination of:

- Strategic and operative aspects of the specific domain of warfare – cyberspace, in this case;
- The specific geopolitical context ongoing while they are drafted;
- Political and strategic goals to be achieved by carrying out a cyber attack;
- Teal response capability of those attacked, cyber warfare capabilities included;

- Any other states and/or third parties that might decide to intervene and/or support the enemy operations, operations in and through the cyberspace included;
- Any reactions from the international community to a counterattack carried out in response to a cyber attack suffered;
- A country's own defence capabilities and especially attack capability in and through the cyberspace.

As per the implementation phase, on the other hand, a country's technical and IT units/agencies play a role of primary importance. Such units must be able to identify in a reasonably short timeframe the source and author of the attack. This, both in case rules of engagement are to be applied as a defence tool but also should a response be needed against a cyber attack.

Here comes the first issue. It is quite easy to reach a very good level of anonymity in cyberspace and it is easy as well to complicate any attempt to attribute responsibility for a cyber attack to its material author or to those who actually ordered the attack.

Further critical elements arise also from the legal point of view. Any response to a cyber attack from a country must mandatorily abide by all the principles of international law, currently applied in case of wars fought in "conventional" warfare domains, *i.e.* land, sea, air, and space.

The principles of necessity, proportionality and distinction are only some of the legal restrictions posed by international law already in force and obviously also applicable to the use states make of IT tools for military purposes. Nevertheless, in practice, it is not always that easy to take into account and comply with such principles.

Finally, a last critical element: cyber attacks are really fast in their final stages, *i.e.* when they are launched against a target and start having effects. Their being so immediate, in fact, presently makes it impossible to follow the OODA (Observe, Orient, Decide, Act) loop, leaving it up to computers and precisely to prearranged engagement rules – already "set" for any different kind of situation – to decide what to do, both in case a defence or a reaction is needed.

It must be easy to guess that, also in light of the two above-mentioned critical elements, arranging rules of engagement for cyberspace presently looks like a particularly complex activity, the outcome of a mix of military, legal, technical and technological competences that are not so easy to be understood and implemented.

Nonetheless, the more and more widespread use of cyberspace as a support tool to military operations and the constant growth in number and quality of cyber attacks – more and more focused on hitting national critical infrastructures – make this need highly topical and absolutely not deferrable, now more than ever.

UNITED STATES

The number of cyber attacks is constantly growing not only in quantity, but especially in quality, considering both the targets being hit, and the complexity and actual objectives of such attacks.

Even leaving out for once cyber espionage threats and cyber warfare, recent news, for instance, clearly show it is long time since propaganda, disinformation and psychological warfare have "made their way" – very effectively, though – thanks to cyberspace, that has by now become one of the main players, also trying to influence the campaign for U.S. elections.

The poor capability to deter (for more details, please see March 2016 "*Cyber Strategy & Policy Brief*"), together with the incapability in coordinating roles, competences and responses to cyber threats, contribute to create a clearly troubling scenario.

To this end, and on the wake of what set forth in the "*Cybersecurity National Action Plan*", published last February (for more details, please see February 2016 "*Cyber Strategy & Policy Brief*"), the recent *Presidential Policy Directive* by President Obama – also known as "PPD-41 - *United States Cyber Incident Coordination*" – is of great interest and spells out the lines of responsibility within the federal government for cyber incident response.

In light of what is set forth in the *Directive*, the U.S. Department of Justice will play a crucial role, acting through the FBI and the *National Cyber Investigative Joint Task Force* as the leading agency responding to threats that might undermine U.S. national or economic interests, international relations, or public health, safety and civil liberties of the American people.

To be clear, threat response activities in this field include not only actions aiming to mitigate threats and facilitate information sharing among the entities involved, but especially carry out real security investigations, collect evidence and gather intelligence in order to provide attribution of a cyber attack by linking related cyber incidents.

On the other hand, the *Department of Homeland Security* (DHS) and especially its *National Cybersecurity and Communications Integration Center* (NCCIC) will be responsible for providing technical assistance to public or private entities hit by a cyber attack. The *Center*, established in 2009 and including US-CERT and ICS-CERT, is responsible for reducing vulnerabilities and their effects, through both purely technical activities, and information sharing and alert to other entities that might face a threat.

Finally, the third pillar of the "*United States Cyber Incident Coordination*" is of course related to intelligence. The *Office of the Director of National Intelligence*, through its *Cyber Threat Intelligence Integration Center*, will be responsible for intelligence support.

It is then clear that the goal of such restructuring is to create a plan to coordinate roles and concentrate efforts, acting through a *Cyber Unified Coordination Group* able to face significant cyber threats that – for dimension, nature or intensity – might undermine U.S. national security and the security of its citizens.

This is a very challenging objective, that – nonetheless – by now proves to be useful and essential, especially in really complex structures, as is the case with U.S., but that is waiting to be examined after entering into force and being effectively implemented.

From the military standpoint, instead, the month of July has seen the request to the U.S. Congress for 2017 cyber security budget. The Secretary of Defense requested 6.7 billion dollars for enhancing cyber capabilities, which is a 900 million increase (15.5%) if compared to 2016.

Thanks to such fund allocation, 2017-2021 U.S. Armed Forces budget for cyber security reaches the considerable amount of 34.6 billion dollars.

Most of these funds will be spent on the protection of the U.S. Department of Defense IT systems and development of capabilities for military operations in and through the cyberspace. For details on developments in the U.S. Armed Forces projects for cyberspace, please see January and March 2016 "*Cyber Strategy & Policy Brief*".

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.*